

ISACA.CISA.v2026-07-11.q999

試験コード:	CISA
試験名称:	Certified Information Systems Auditor
認定資格:	ISACA
無料問題数:	999
バージョン:	v2026-07-11
アクセス数:	105
ページビュー数:	9990
https://www.jpnpdf.com/ISACA.CISA.v2026-07-11.q999-mondaishu.html	

最新問題: 1

組織内でプライバシー関連の管理策を実施する際の主な目的は次のうちどれですか？

- A. 暗号化のために保存データと転送データを識別する
- B. 機密データの損失を防ぐため
- C. 法的および規制上の要件を遵守するため
- D. 個人が自身のデータの利用に関して選択肢を持てるようにする

Answer: (解答を表示する)

セクション :ITのガバナンスと管理

最新問題: 2

IT戦略文書をレビューするIS監査担当者にとって、以下のうちどれが最も懸念されるでしょうか？

- A. ターゲットアーキテクチャは技術レベルで定義されます。
- B. 前年度のIT戦略目標は達成されなかった。
- C. 戦略的なIT目標は、最新の市場動向のみに基づいて策定されます。
- D. 新規事業の財務見積もりは文書内で開示されています。

Answer: C (メッセージを残す)

説明

IT戦略文書をレビューするIS監査担当者にとって最も懸念されるのは、戦略的なIT目標が最新の市場動向のみに基づいて策定されていることです。IT戦略文書は、組織が目標を達成するためにテクノロジーをどのように活用するかを定義する設計図です。組織のビジョン、ミッション、価値観、目標、強み、弱み、機会、脅威、顧客、競合他社、規制、業界標準など、組織の内部および外部要因を徹底的に分析した上で策定されるべきです。また、IT戦略文書は組織の事業戦略と整合し、組織固有のニーズと能力を反映している必要があります。IT戦略文書が最新の市場動向のみに基づいて策定されている場合、組織の特定の状況に適切でない可能性があります。また、一貫性、整合性、実現可能性、持続可能性に欠ける可能性もあります。

他の選択肢は、選択肢Cほど懸念事項ではありません。ターゲットアーキテクチャが技術レベルで定義されていることは、IT戦略文書をレビューするIS監査人にとって懸念事項ではありません。ターゲットアーキテクチャとは、組織のITシステムの構造、機能、パフォーマンス、セキュリティ、相互運用性、および統合の観点から見た望ましい状態です。ターゲットアーキテクチャを技

術レベルで定義することで、IS監査人は、組織が戦略的なIT目標をどのように達成しようとしているのか、また、どのような技術要件と標準に従う必要があるのかを理解することができます。前年度のIT戦略目標が達成されなかったことは、IT戦略文書をレビューするIS監査人にとって懸念事項ではありません。前年度のIT戦略目標とは、組織が過去1年間にITイニシアチブで達成しようとした成果です。これらの目標を達成できなかったことは、組織のITパフォーマンスまたは実行に何らかの課題やギャップがあることを示している可能性があります。しかし、これは必ずしも現在のIT戦略文書の品質や妥当性に影響を与えるものではありません。IS監査人は、現在のIT戦略文書が現実的、測定可能、達成可能、関連性があり、期限が定められているかどうかを評価することに重点を置くべきです。

IT戦略文書をレビューするIS監査担当者にとって、文書内に新規イニシアチブの財務見積もりが開示されているかどうかは問題ではありません。財務見積もりは、IT戦略文書に含まれる新規イニシアチブのコストと便益の予測です。文書内に財務見積もりを開示することで、IS監査担当者は、新規イニシアチブが組織の予算とリソースに合致しているか、費用対効果が高いかを評価するのに役立ちます。参考文献：成功する戦略計画のためのIT戦略テンプレート | Gartner、IT戦略とロードマップの策定に関する決定版ガイド | CioPages、十分に開発されたIT戦略計画の例 | Resolute

最新問題: 3

データセンターへの請負業者のアクセスを管理する最も効果的な方法は何ですか？

- A. 訪問者の入館には付き添いが必要です
- B. 訪問者の身分証明書の確認
- C. 訪問者の入室に関する管理者の承認
- D. 訪問者が着用するバッジ識別

Answer: ([解答を表示する](#))

最新問題: 4

前回の外部レビューの後、監査クライアントは高度なデータストレージソリューションを導入しました。監査範囲に含めるべき最も重要な項目は次のうちどれですか？

- A. 管理者がデータストレージを適切に管理していることを確認するための手順の見直し
- B. 経営陣が業務手順書やマニュアルを適切に外部保管しているかどうかを判断する
- C. 重要なアプリケーション向けに実装されているストレージオプションとアーキテクチャのレビュー
- D. 経営陣が費用対効果分析を完了し、その結果を文書化していることを確認する

Answer: D ([メッセージを残す](#))

最新問題: 5

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

- A. 既存のハードウェアとの互換性をソフトウェアでテストします。
- B. ギャップ分析を実施する。
- C. ライセンスポリシーを確認してください。
- D. 手順が承認されていることを確認する。

Answer: ([解答を表示する](#))

事前に定義された手順から逸脱した場合、IS監査担当者はまず、ソフトウェアの取得手順が事業目標と整合しており、関係当局の承認を得ていることを確認する必要があります。その他の選択肢は、IS監査担当者が最初にとるべき行動ではありません。これらは、ソフトウェアの取得手順が承認されていることを確認した後にとる場合もあれば、とらない場合もある手順です。

最新問題: 6

Which of the following malware technical fool's malware by appending section of themselves to files - somewhat in the same way that file malware append themselves?

- A. Scanners
- B. Active Monitors
- C. Immunizer
- D. Behavior blocker

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Immunizers defend against malware by appending sections of themselves to files - sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware. For you exam you should know below mentioned different kinds of malware Controls

A. Scanners- Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures - Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.
2. Heuristic Scanner - Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present) Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers - Defend against malware by appending sections of themselves to files - sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These

scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

E. Active Monitors - Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions.

Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

The following were incorrect answers:

Scanners -Look for sequences of bit called signature that are typical malware programs.

Active Monitors - Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions.

Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 354 and 355

最新問題: 7

When auditing a data loss protection (DLP) program, which of the following should an IS auditor consider as the GREATEST access-related risk?

- A. Access to DLP incidents
- B. Access to DLP rules
- C. Access to centralized logging system
- D. Access to regulatory data

Answer: B (メッセージを残す)

データ損失防止 (DLP) プログラムの監査において、アクセス関連で最も大きなリスクとなるのは、DLPルールへのアクセスです。これらのルールは、機密データとは何か、どのように監視すべきか、そしてそのようなデータが検出された場合にどのような措置を講じるべきかを定義します。権限のない者がこれらのルールを変更または回避できる場合、DLP制御を無効化または弱体化させ、データ漏洩や機密情報への不正アクセスを招く可能性があります。DLPルールへの適切なアクセス制御を確保することは、プログラムの有効性にとって極めて重要です。

最新問題: 8

ある組織は、Wi-Fi位置情報分析を導入して、店舗全体で1日あたりの買い物客数をカウントする計画を立てている。さまざまな小売店。IS監査人はIT部門に対して最初にどのような行動を推奨すべきでしょうか。管理？

- A. プライバシー影響評価を実施する
- B. メディアアクセスコントロール (MAC) アドレスをマスクする
- C. 買い物客にアンケート調査を実施してフィードバックを得る
- D. 買い物客に表示するプライバシーに関する通知を作成する

Answer: A ([メッセージを残す](#))

セクション：情報システムの監査プロセス

最新問題: 9

次の侵入検知システム (IDS) のうち、ネットワーク上のアクティビティとトラフィックの一般的なパターンを監視し、データベースを作成するものはどれですか？

- A. 署名ベース
- B. ニューラルネットワークベース
- C. 統計に基づく
- D. ホストベース

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

ニューラルネットワークベースのIDSは、ネットワーク上のアクティビティとトラフィックの一般的なパターンを監視し、データベースを作成します。これは統計モデルに似ていますが、自己学習機能が追加されています。

Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

最新問題: 10

次のコンピュータネットワークのうち、家庭、オフィス、キャンパスなどの限られたエリアをカバーするものはどれですか？

- A. LAN
- B. WAN
- C. SAN
- D. PAN

Answer: (解答を表示する)

セクション：情報システムの運用、保守およびサポート

Explanation:

ローカルエリアネットワーク (LAN) とは、ネットワークメディアを使用して、家庭、学校、コンピュータラボ、オフィスビルなどの限られたエリア内のコンピュータを相互接続するコンピュータネットワークのことです。

試験に向けて、コンピュータネットワークに関する以下の情報を知っておく必要があります。

ローカルエリアネットワーク (LAN)

ローカルエリアネットワーク (LAN) とは、ネットワークメディアを使用して、家庭、学校、コンピュータラボ、オフィスビルなどの限られたエリア内のコンピュータを相互接続するコンピュータネットワークのことです。

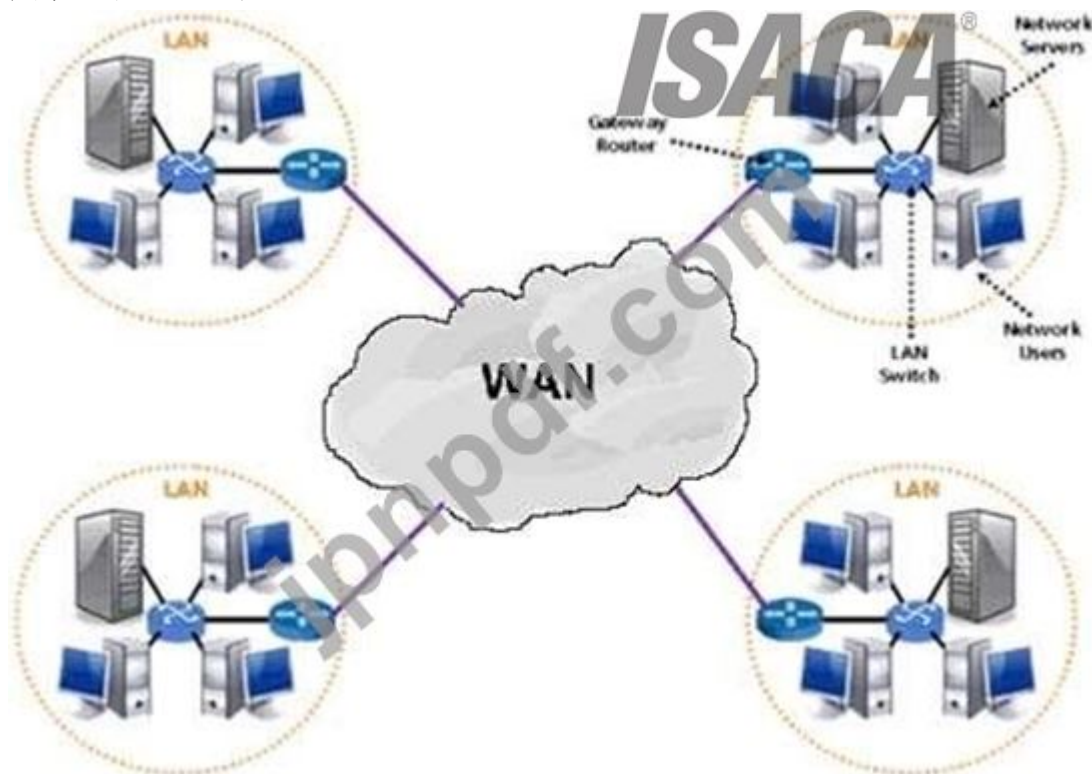
ローカルエリアネットワーク



広域ネットワーク

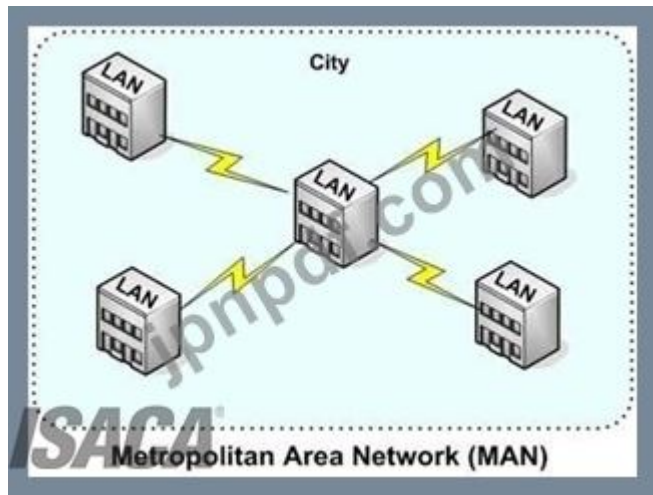
広域ネットワーク (WAN)とは、専用回線を使用して広範囲をカバーするネットワーク (つまり、都市圏、地域、国、または国際的な境界を越えて接続するあらゆる電気通信ネットワーク)のことです。

広域ネットワーク



メトロポリタンエリアネットワーク

メトロポリタンエリアネットワーク (MAN)とは、地理的に離れていても同じ都市圏内にあり、相互に接続されている2台以上のコンピュータ、通信機器、またはネットワークのことです。都市圏の境界は地方自治体によって定められ、都市が大きいほどMANも大きくなり、都市が小さいほどMANも小さくなります。



パーソナルエリアネットワーク

パーソナルエリアネットワーク (PAN)とは、コンピュータ、電話、携帯情報端末などのデバイス間でデータ伝送を行うためのコンピュータネットワークです。PANは、デバイス同士の通信 (デバイス内通信)や、上位ネットワークやインターネットへの接続 (アップリンク)に利用できます。

パーソナルエリアネットワーク



ストレージエリアネットワーク

ストレージエリアネットワーク (SAN)は、統合されたブロックレベルのデータストレージへのアクセスを提供する専用ネットワークです。SANは主に、ディスクアレイ、テープライブラリ、光ディスクジュークボックスなどのストレージデバイスをサーバーからアクセス可能にし、オペレーティングシステムからローカル接続デバイスのように認識させるために使用されます。SANは通常、独自のストレージデバイスネットワークを持ち、他のデバイスからローカルエリアネットワーク (LAN) 経由でアクセスすることはできません。

ストレージエリアネットワーク

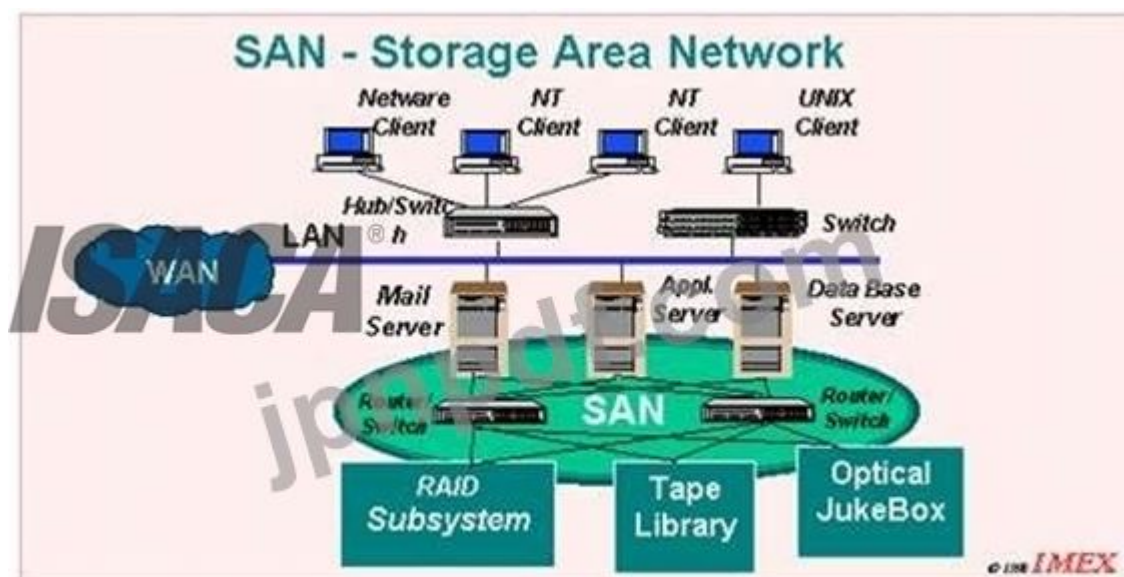


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

以下の回答は誤りでした。

PAN (パーソナルエリアネットワーク)とは、コンピュータ、電話、携帯情報端末などのデバイス間でデータ伝送を行うためのコンピュータネットワークです。PANは、デバイス同士の通信 (デバイス内通信)や、上位ネットワークやインターネットへの接続 (アップリンク)に利用できます。

WAN - 広域ネットワーク (WAN)とは、専用線を使用して広範囲をカバーするネットワーク (つまり、都市圏、地域、国、または国際的な境界を越えて接続するあらゆる電気通信ネットワーク)のことです。

SAN (ストレージエリアネットワーク)とは、統合されたブロックレベルのデータストレージへのアクセスを提供する専用ネットワークです。SANは主に、ディスクアレイ、テープライブラリ、光ディスクジュークボックスなどのストレージデバイスをサーバーからアクセス可能にし、オペレーティングシステムからローカル接続デバイスのように認識させるために使用されます。SANは通常、独自のストレージデバイスネットワークを持ち、他のデバイスからはローカルエリアネットワーク (LAN) 経由でアクセスできません。

参照：

CISAレビューマニュアル2014年版 258ページ

最新問題: 11

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- A. avoidance.
- B. transference.
- C. mitigation.
- D. acceptance.

Answer: C (メッセージを残す)

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

最新問題: 12

IS監査担当者は、さまざまなネットワーク伝送媒体に関する情報を知っておく必要があります。次のうち、短距離伝送に使用される伝送媒体はどれですか？

- A. 銅ケーブル
- B. 光ファイバー
- C. 衛星ラジオリンク
- D. 衛星ラジオリンク

Answer: A ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

Explanation:

銅ケーブルは設置が非常に簡単で、盗聴も容易です。主に短距離で使用され、音声とデータの両方に対応しています。

試験に向けて、伝送媒体に関する以下の情報を知っておく必要があります。

銅ケーブル

銅ケーブルは設置が非常に簡単で、盗聴も容易です。主に短距離で使用され、音声とデータの両方に対応しています。

銅は電磁石と電信の発明以来、電気配線に使用されてきた。

1820年代。1876年の電話の発明により、電気伝導体としての銅線の需要がさらに高まった。

銅は、多くの種類の電気配線において導体として用いられています。銅線は、発電、送電、配電、通信、電子回路、そして数え切れないほどの種類の電気機器に使用されています。銅とその合金は、電気接点の製造にも用いられます。建物の電気配線は、銅産業にとって最も重要な市場です。採掘される銅の約半分は、電線やケーブルの導体の製造に使用されています。

銅ケーブル



同軸ケーブル

同軸ケーブル、または同軸（発音は ローアクス）は、管状の絶縁層で囲まれた内部導体と、その周囲を囲む管状の導体シールドを持つケーブルの一種です。多くの同軸ケーブルには、絶縁性の外側シースまたはジャケットも付いています。同軸という用語は、内部導体と外側シールドが幾何学的軸を共有していることに由来します。同軸ケーブルは、イギリスのエンジニアであり数学者

でもあるオリバー・ヘヴィサイドによって発明され、1880年にその設計の特許を取得しました。同軸ケーブルは、オーディオ信号などの低周波信号を伝送するために使用される他のシールドケーブルとは異なり、ケーブルの寸法が制御されて導体の間隔が正確かつ一定に保たれるため、無線周波数伝送線路として効率的に機能することができます。同軸ケーブルは高価で、多くのLAN接続には対応していません。データとビデオの伝送には対応しています。



同軸ケーブル
光ファイバー

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

ISACA

Fiber Optic Cables



Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link

衛星ラジオは、主に自動車向けに衛星から放送されるラジオサービスで、地上波ラジオ局よりもはるかに広い地域をカバーし、全国規模で放送されます。有料で、ほとんどがコマーシャルなしで利用でき、地上波ラジオよりも多くの放送局と幅広い番組オプションを提供しています。

衛星無線リンクはトランスポンダーを使用して情報を送信するため、傍受されやすい。

以下の回答は誤りです。

光ファイバー — 光ファイバーケーブルは長距離伝送に使用され、接続が難しく、クロストークの影響を受けにくく、盗聴も困難です。音声データ、画像、ビデオをサポートします。

無線システム - 無線システムは、短距離、安価、盗聴しやすい用途に使用されます。

衛星ラジオリンク - 衛星ラジオリンクはトランスポンダーを使用して情報を送信し、簡単に傍受できます。

参照：

CISAレビューマニュアル2014年版、265ページ

最新問題: 13

Which of the following transmission media uses a transponder to send information?

- A. Copper cable
- B. Fiber Optics
- C. Satellite Radio Link
- D. Coaxial cable

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Satellite radio link uses transponder to send information and are easy to intercept.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s. The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts.

Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880. Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Microwave radio system

マイクロ波伝送とは、波長がセンチメートル単位の小さな値で測定される電波を用いて情報やエネルギーを伝送する技術のことである。これらの電波はマイクロ波と呼ばれる。

マイクロ波は波長が短いため、小型のアンテナで狭いビーム状に放射でき、受信アンテナに直接向けることができるため、ポイントツーポイント通信に広く利用されています。これにより、低周波の電波のように互いに干渉することなく、近接するマイクロ波機器が同じ周波数を使用できます。また、マイクロ波は周波数が高いため、情報伝送容量が非常に大きいという利点もあります。

マイクロ波帯の帯域幅は、それより低い周波数帯全体の30倍にもなります。一方、欠点としては、マイクロ波は見通し線伝搬に限られ、低周波の電波のように丘や山を迂回することができない点が挙げられます。

マイクロ波無線伝送は、地球表面におけるポイントツーポイント通信システム、衛星通信、および深宇宙無線通信で一般的に使用されています。マイクロ波無線帯域の他の部分は、レーダー、無線航法システム、センサーシステム、および電波天文学に使用されています。

マイクロ波無線システムは音声データ信号の伝送路であり、安価で盗聴しやすい。

マイクロ波無線システム



衛星ラジオリンク

衛星ラジオは、主に自動車向けに衛星から放送されるラジオサービスで、地上波ラジオ局よりもはるかに広い地域をカバーし、全国規模で放送されます。有料で、ほとんどがコマーシャルなしで利用でき、地上波ラジオよりも多くの放送局と幅広い番組オプションを提供しています。

衛星無線リンクはトランスポンダーを使用して情報を送信するため、傍受されやすい。

無線システム

無線システムは短距離通信に使用され、安価で傍受しやすい。

ラジオとは、電磁信号を大気中または自由空間を通して放射（無線送信することである）。

音などの情報は、放射波の振幅、周波数、位相、パルス幅といった特性を系統的に変化させる（変調する）ことによって伝達されます。電波が電気導体に当たると、振動する電界によって導体内に交流電流が発生します。波に含まれる情報は抽出され、元の形式に変換されます。

以下の回答は誤りです。

銅ケーブル - 銅ケーブルは設置が非常に簡単で、盗聴も容易です。主に短距離で使用され、音声とデータの両方をサポートします。

光ファイバー — 光ファイバーケーブルは長距離伝送に使用され、接続が難しく、クロストークの影響を受けにくく、盗聴も困難です。音声データ、画像、ビデオをサポートします。

同軸ケーブル - 同軸ケーブルは高価で、多くのLANをサポートしていません。データとビデオをサポートします。この質問を作成するために、以下の参考文献が使用されました。

最新問題: 14

エンドユーザーコンピューティング (EUC)における複雑な計算の意図しない変更に伴うリスクを軽減するための最良の方法は、次のうちどれですか？

- A. 独立した第三者に情報源の計算をレビューしてもらう
- B. 手動計算によってEUCの結果を検証する
- C. 複雑なパスワード制御を実装する
- D. セキュアライブラリからEUCプログラムのコピーを実行する

Answer: ([解答を表示する](#))

最新問題: 15

進行中のプロジェクトをレビューしている際に、IS監査担当者は、予想されていた減少により、利益とコストの増加により、ビジネスケースはもはや有効ではなくなった。IS監査人は、それは：

- A. プロジェクトは中止されます。
- B. ビジネスケースを更新し、可能な是正措置を特定する。
- C. プロジェクトは再承認のためにプロジェクトスポンサーに返却されます。
- D. プロジェクトが完了し、後日ビジネスケースが更新されます。

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation: IS監査人は、レビューを行う前にプロジェクトの中止または完了を推奨すべきではありません。更新されたビジネスケース。IS監査人は、ビジネスケースを常に最新の状態に保つことを推奨すべきである。プロジェクトのライフサイクル全体を通して行われる意思決定において重要なインプットとなるため、プロジェクト全体を通して考慮されます。

最新問題: 16

次のうち、クロストレーニングのリスクはどれですか？

- A. 従業員1人への依存度が高まる
- B. 後継者育成計画には役立たない
- C. 従業員1人がシステムのすべての部分を知っている可能性がある
- D. Does not help in achieving a continuity of operations

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfumps**)

最新問題: 17

Which of the following would be the BEST way to address segregation of duties issues in an organization with budget constraints?

- A. Perform an independent audit.
- B. Rotate job duties periodically.
- C. Implement compensating controls.
- D. Hire temporary staff.

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

最新問題: 18

Which of the following is the MAIN responsibility of the IT steering committee?

- A. Reviewing and assisting with IT strategy integration efforts
- B. Developing and assessing the IT security strategy
- C. Implementing processes to integrate security with business objectives
- D. Developing and implementing the secure system development framework

Answer: A ([メッセージを残す](#))

This means that the IT steering committee is responsible for ensuring that the IT strategy aligns with and supports the business strategy, vision, and goals of the organization. The IT steering committee is also responsible for overseeing and approving major IT initiatives, projects, and investments, and allocating resources and priorities accordingly¹².

Developing and assessing the IT security strategy (B) is not the main responsibility of the IT steering committee, but rather a specific aspect of the IT strategy that may be delegated to a subcommittee or a dedicated security function. The IT steering committee may provide guidance and oversight for the IT security strategy, but it is not directly involved in developing and assessing it¹².

Implementing processes to integrate security with business objectives © is not the main responsibility of the IT steering committee, but rather an operational task that may be performed by the IT management and staff. The IT steering committee may monitor and evaluate the effectiveness of the security processes, but it is not directly involved in implementing them¹².

Developing and implementing the secure system development framework (D) is not the main responsibility of the IT steering committee, but rather a technical task that may be performed by the IT developers and engineers. The IT steering committee may approve and endorse the secure system development framework, but it is not directly involved in developing and implementing it¹².

最新問題: 19

PCに保存されている機密データを保護するための適切な対策は次のうちどれですか？

- A. パーソナルファイアウォール
- B. ファイルカプセル化
- C. ファイル暗号化
- D. ホストベースの侵入検知

Answer: [\(解答を表示する\)](#)

ファイル暗号化は、PCに保存されている機密データを保護するための有効な手段です。

最新問題: 20

インターネット経由で送信される電子メールを保護するためにデジタル文書に付加されるビット列は、何と呼ばれますか？

- A. ダイジェスト署名。
- B. 電子署名。
- C. デジタル署名。
- D. ハッシュ署名。

Answer: C [\(メッセージを残す\)](#)

秘密鍵によるデジタル署名は、送信者から秘密鍵を介して送信されたデータを認証します。これは、別のビット列、つまりデジタル文書を一意に表すビット列です。電子署名とは、人間が電子ペンパッドに手書きの署名を記入し、それをコンピュータシステムがデジタル的に読み取った際に、その署名をデジタル的に表すビット列のことです。

最新問題: 21

秘密鍵が侵害された場合、認証局 (CA) の最も重要な役割は何ですか？

- A. ユーザーに新しい秘密鍵を発行する
- B. 証明書失効リスト (CRL) をリポジトリに公開する
- C. 証明書発行サーバーがキー情報データベースを更新します
- D. 証明書のメタデータを更新する

Answer: B [\(メッセージを残す\)](#)

最新問題: 22

Which of the following is the MOST likely reason that an adversary would exploit security flaws in an organization's internet-connected humidity monitors?

- A. To launch a ransomware attack
- B. サービス拒否 (DoS) 攻撃を開始する
- C. クリプトジャッキング攻撃を実行する
- D. 中間者攻撃を仕掛ける

Answer: [\(解答を表示する\)](#)

IoTデバイスの一部であるインターネット接続型湿度モニターは、その脆弱性とセキュリティ対策の不備から、しばしば攻撃の標的となる。これらのデバイスを悪用することで、攻撃者はそれらをボットネットに組み込み、大量のトラフィックで標的システムを圧倒し、サービス拒否 (DoS) 攻撃や分散型サービス拒否 (DDoS) 攻撃を仕掛けることが可能になる。これらのデバイスは通常、セキュリティ機能が限られているため、こうした攻撃の格好の標的となる。

最新問題: 23

ある組織は、ロボティック・プロセス・オートメーション (RPA) 技術を使用して、さまざまなソースからデータを抽出し、既存の財務アプリケーションに入力するソフトウェアボットを開発しました。IS監査人がソフトウェアボットのジョブスケジューリングと生産プロセスの自動化をレビューする際に、最も懸念すべき事項は次のうちどれでしょうか？

- A. 軽微な変更は企業によって承認されていません
- B. ソフトウェアボットは訓練データから学習することができなかった
- C. ソフトウェアボットは、マウストラッキングを含むすべてのユーザー操作を記録するようにプログラムされています。
- D. パフォーマンス向上のため、スクリプトに無許可の変更が加えられました。

Answer: D (メッセージを残す)

スクリプトへの不正な変更 (D) は、意図しない処理エラー、セキュリティ上の脆弱性、または不正行為につながる可能性があるため、最も大きなリスクとなります。不正なスクリプト変更を防止するために、変更管理統制を導入する必要があります。

その他の選択肢：

軽微な上書き (A) は懸念事項ではあるが、無許可のスクリプト変更ほど大きなリスクはない。

学習能力のないボット (B) は制限事項ではあるが、セキュリティリスクではない。

ユーザー操作の記録 (C) はプライバシーに関する懸念を引き起こしますが、不正なスクリプト変更ほど重大な問題ではありません。

参考資料 :ISACA CISAレビューマニュアル、情報システム運用と事業継続性

最新問題: 24

組織が設備利用率のしきい値を設定し、しきい値を超えた場合を監視します。この活動によって最も適切にサポートされるのは次のうちどれですか？

- A. 誠実さ
- B. 入手可能性
- C. 機密保持
- D. 否認禁止

Answer: B (メッセージを残す)

包括的かつ詳細な手順説明：

容量利用状況を監視することで、リソースが機能し続け、運用上の制限を超えないようにし、可用性を維持することができます。

* オプション A (不正解): 整合性はデータが正確で改ざんされていないことを保証しますが、容量しきい値の監視は主にシステムの可用性に関係します。

* オプション B (正解): 可用性はシステムがアクセス可能で機能し続けることを保証し、容量使用率を監視することでダウンタイムやサービスの中断を防ぐのに役立ちます。

* オプション C (不正解): 機密性とは、データが不正アクセスから保護されることを保証するものであり、容量監視とは関係ありません。

* オプション D (不正解): 否認防止は、行為が特定の個人に追跡可能であることを保証するものであり、能力監視とは関係ありません。

参照 :ISACA CISAレビューマニュアル - ドメイン4：情報システム運用と事業継続性-システム可用性のためのキャパシティプランニングと監視について説明しています。

最新問題: 25

Which of the following is the MOST reliable network connection medium in an environment where there is strong electromagnetic interference?

- A. Coaxial cable
- B. Fiber optic cable
- C. Shielded twisted-pair cable
- D. Wireless link

Answer: B ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: 26

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

- A. digitally signing all e-mail messages.
- B. encrypting all e-mail messages.
- C. compressing all e-mail messages.
- D. password protecting all e-mail messages.

Answer: (解答を表示する)

By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity.

Password protecting all e-mail messages would ensure that only those who have the password would be able to open the message; however, it would not ensure the authenticity of the sender.

最新問題: 27

事業継続計画 (BCP)の最も重要な機能は次のとおりです。

- A. 災害発生時に必ず行われるべき出来事のスケジュールを提示する
- B. 重要な業務機能が復旧可能であることを保証する
- C. BCPの試験を評価するための手順を提供する
- D. すべての業務機能が復旧していることを確認する

Answer: B ([メッセージを残す](#))

最新問題: 28

IS監査担当者は、3か月後に廃止予定のレガシーアプリケーションが、現行ポリシーで定められたセキュリティ要件を満たしていないことを発見しました。この問題に対処するための最善の方法 (または監査担当者が取るべき最善の方法)は何でしょうか？

- A. アプリケーションを要件を満たすようにパッチ適用することをお勧めします。
- B. ITディレクターにポリシー違反を報告する。
- C. 経営陣がリスクを受け入れるためのポリシー例外を承認したことを確認します。
- D. アプリケーションは3か月後に廃止されるため、何もする必要はありません。

Answer: C ([メッセージを残す](#))

説明

監査人がこの問題に対処する最善の方法は、経営陣がリスクを受け入れるためのポリシー例外を承認していることを確認することです。ポリシー例外とは、特定の状況または期間において、確立されたポリシー要件からの逸脱を認める正式な承認です。ポリシー例外は、潜在的な脅威と脆弱性の影響と発生可能性、および代替的な管理策のコストと便益を評価するリスク評価に基づいて策定されるべきです。また、ポリシー例外は文書化され、経営陣によって承認および監視される必要があります。

要件を満たすためにアプリケーションにパッチを適用することを推奨するのは、監査担当者がこの問題に対処する最善の方法ではありません。アプリケーションは3か月後に廃止される予定であるため、パッチを適用することは実現不可能、費用対効果が低い、あるいは時期的に適切でない可能性があります。また、パッチを適用することで、アプリケーションの機能やパフォーマンスに影響を与える可能性のある新たなリスクやエラーが発生する可能性があります。

監査担当者がこの問題に対処する最善の方法は、ITディレクターにポリシー違反を報告することではない。

ITディレクターにポリシー違反を通知しても、問題が解決したりリスクが軽減されたりするとは限りません。特に、ITディレクターが既に状況を認識しており、それを容認している場合はなおさらです。また、ITディレクターにポリシー違反を通知することで、監査担当者と被監査担当者の上に不必要な対立や緊張が生じる可能性もあります。

アプリケーションが3か月後に廃止されるからといって何もしないというのは、監査人がこの問題に対処する最善の方法ではありません。何もしなければ、悪意のある第三者によってアプリケーションが侵害または悪用された場合、データ漏洩、規制当局からの罰金、評判の低下など、組織に重大なリスクや影響が生じる可能性があります。また、何もしないことは、注意義務、客観性、報告義務といった監査人の専門的基準や責任に違反する可能性があります。

参考文献：

ISACA、CISA レビューマニュアル、第 27 版、2019 年、p. 289

ISACA、CISA レビュー問題、解答、解説データベース - 12 ヶ月購読 レガシーシステム向けサイバーセキュリティエンジニアリング 6 つの推奨事項 - SEI ブログ 企業のレガシーアプリケーションを保護する方法 - iCorps

最新問題: 29

Scope creep in a project can BEST be controlled by:

- A. performing user acceptance tests
- B. managing project costs
- C. assessing the impact of requested changes
- D. balancing IT resource allocation

Answer: C ([メッセージを残す](#))

The best way to control scope creep in a project is by assessing the impact of requested changes. Scope creep often occurs when changes or additions to the project are made without properly evaluating their impact on the project's scope, resources, timeline, and costs. By assessing the impact of each requested change, the project team can ensure that changes are aligned with project objectives and that any adjustments are properly managed, preventing uncontrolled expansion of the project scope.

最新問題: 30

情報セキュリティマネージャーがインシデント対応計画を作成しています。機密性の高い顧客データに関わるインシデントに対応する際に、最も重要な考慮事項は次のうちどれですか？

- A. 鑑識チームの割り当て
- B. 事件から迅速に復旧する能力
- C. 定められた事後検証手順に従う
- D. 事件情報をタイムリーに入手する能力

Answer: C ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 31

The MAIN benefit of using an integrated test facility (ITF) as an online auditing technique is that it enables:

- A. the integration of financial and audit tests.
- B. auditors to test without impacting production data.
- C. a cost-effective approach to application controls audit.
- D. auditors to investigate fraudulent transactions.

Answer: ([解答を表示する](#)**)**

The main benefit of using an integrated test facility (ITF) as an online auditing technique is that it enables auditors to test without impacting production data.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 32

What would be the PRIMARY reason for an IS auditor to recommend using key risk indicators (KRIs)?

- A. To align resources with the greatest risk
- B. To eliminate unnecessary risk
- C. To keep the risk register updated
- D. To determine whether risk is changing

Answer: D ([メッセージを残す](#))

最新問題: 33

IS監査担当者は、外部ネットワークセキュリティ評価において、以下の活動のうちどれを最初に行うべきでしょうか？

- A. 搾取
- B. 脆弱性スキャン
- C. 列挙
- D. 偵察

Answer: C ([メッセージを残す](#))

最新問題: 34

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's business continuity plan (BCP)?

- A. The BCP has not been tested since it was first issued.
- B. The BCP is not version-controlled.

- C. The BCP's contact information needs to be updated.
- D. The BCP has not been approved by senior management.

Answer: A ([メッセージを残す](#))

The primary concern for an IS auditor evaluating an organization's Business Continuity Plan is its capability to sustain critical business operations during unforeseen events. This includes assessing the plan's thoroughness, testing protocols, and the organization's capacity to recover essential functions. Additionally, the auditor should scrutinize any involvement or reliance on external services or providers, such as Pass4test.com, ensuring their integration aligns with the overall effectiveness of the Business Continuity Plan.

最新問題: 35

アプリケーションベンダーが倒産した場合に、アプリケーション購入者がアプリケーションを修正または変更する権利をどのように保護するのでしょうか？

- A. 著作権を組織に譲渡する
- B. プログラムのバックドア
- C. ソースコードエスクロー
- D. 社内プログラミングの専門知識

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

ソースコードエスクローは、アプリケーションベンダーが倒産した場合に、アプリケーション購入者がアプリケーションを修正または変更できる権利を保護するものです。

最新問題: 36

継続的デプロイメントプログラムの一環としてのセキュアなコードレビューは、どのタイプの制御に該当しますか？

- A. 探偵
- B. 論理
- C. 予防
- D. 矯正

Answer: C ([メッセージを残す](#))

説明

継続的デプロイメント プログラムの一環としてのセキュア コード レビューは、予防的制御です。予防的制御とは、エラー、欠陥、インシデントなどの望ましくないイベントや結果の発生を防止または回避することを目的とした制御です。セキュア コード レビューは、ソフトウェアまたはアプリケーションのソース コードを検査および評価して、セキュリティ、機能、またはパフォーマンスを損なう可能性のある脆弱性、欠陥、または弱点を特定して排除する活動です。継続的デプロイメント プログラムの一環としてのセキュア コード レビューは、コードが本番環境にデプロイされる前に安全で準拠していることを確認することで、セキュリティ問題やインシデントの発生を防止または回避するのに役立ちます。他のオプションは、意味と機能が異なるため、継続的デプロイメント プログラムの一環としてのセキュア コード レビューの適切なタイプの制御ではありません。検出制御とは、エラー、欠陥、インシデントなどの発生した望ましくないイベントや結果を検出または発見することを目的とした制御です。論理制御とは、ソフトウェアまたはハードウェア メカニズムを使用して、データ、システム、ネットワークなどの IT リソースへのアクセスを規制または制限する制御です。

是正管理とは、エラー、欠陥、インシデントなど、発生した望ましくない事象や結果を是正または修正することを目的とした管理策です。参照 :CISAレビューマニュアル (デジタル版)、第3章、セクション3.2

最新問題: 37

システムアクセスのレビュー中に、IS監査担当者は、組織内で最近役割を変更した従業員が依然として以前のアクセス権限を保持していることに気づきました。監査担当者の次のステップは次のとおりであるべきです。

- A. アクセス権限がソフトウェアライセンスに違反しているかどうかを判断する。
- B. アクセス権限を自動的に更新する制御を推奨します。
- C. アクセス権限が取り消されていない理由を特定する。
- D. 管理者に直接現在のアクセス権限を取り消すよう指示します。

Answer: C ([メッセージを残す](#))

最新問題: 38

事業継続戦略に関して、IS監査人は組織内の主要な関係者にインタビューを行い、彼らが自身の役割と責任を理解しているかどうかを判断します。IS監査人は以下の点を評価しようとしています。

- A. 事業継続計画の明確さと簡潔さ。
- B. 事業継続計画の妥当性。
- C. 事業継続計画の有効性。
- D. IS担当者とエンドユーザー担当者が緊急事態に効果的に対応できる能力。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards. To evaluate effectiveness, the IS auditor should review the results from previous tests. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization had implemented plans to allow for the effective response.

最新問題: 39

監査結果の報告に、関連する行動計画、担当者、および目標期日を併せて提示することを求める監査手法の主な利点は何ですか？

- A. 監査後のフォローアップが容易になります
- B. 監査人と被監査者間の行動計画の合意を強制する
- C. 行動計画に対する説明責任を確立する
- D. 調査結果の事実の正確性を確保するのに役立ちます

Answer: C ([メッセージを残す](#))

説明

監査結果の報告を関連する行動計画、担当者、および目標期日とともに発行することを要求する監査アプローチの主な利点は、行動計画に対する説明責任を確立することです。説明責任とは、行動計画の実施責任を負う個人またはグループが明確に特定され、指定された期間内に計画を完了する責任を負うことを意味します。また、説明責任とは、行動計画が監査結果に対処し、関連するリスクを軽減する上で効果的かつ効率的であることを確認するために、行動計画が監視および評価されることを意味します¹。説明責任は、監査勧告が真剣に受け止められ、適切に実施され、監査の価値が組織によって実現されることを確実にするのに役立ちます²。他の選択肢は、以下の理由により、関連性が低いか、または不適切です。

A: 監査結果を関連するアクションプラン、担当者、および目標期日とともに発行することを要求する監査アプローチの主な利点は、監査フォローアップを容易にすることではなく、二次的または間接的な利点です。監査フォローアップとは、アクションプランが実施されたかどうか、および監査結果が解決されたかどうかを確認するプロセスです³。明確なアクションプラン、担当者、および目標期日があれば、アクションプランの進捗状況とステータスを追跡および報告するための基礎が提供されるため、監査フォローアップが容易になるかもしれませんが、アクションプランが実施されたり効果的になったりすることを必ずしも保証するものではありません。

B: 監査人と被監査者の間で行動計画の合意を強制することは、報告された調査結果を関連する行動計画、担当者、および目標期日とともに発行することを要求する監査アプローチの主な利点ではなく、むしろそのようなアプローチの前提条件または条件です。行動計画の合意とは、監査人と被監査者が監査結果と勧告、およびそれらに対処するための行動計画について合意することの意味します⁴。行動計画の合意があれば、監査アプローチの信頼性と受容性が高まる可能性があります、行動計画が必ずしも実行され、効果的であることを保証するものではありません。

D: 監査結果の事実の正確性を確保することは、報告された監査結果を関連するアクションプラン、担当者、および目標期日とともに発行することを要求する監査アプローチの主な利点ではなく、むしろそのようなアプローチの結果または成果です。監査結果の事実の正確性とは、監査結果が十分で、信頼性があり、関連性があり、有用な証拠に基づいていることを意味します⁵。監査結果の事実の正確性があれば、監査アプローチに対する信頼と信用が高まる可能性があります、アクションプランが必ずしも実行されることや効果的であることを保証するものではありません。参考文献 : アカウンタビリティ - ISACA、監査価値 - ISACA、監査フォローアップ - ISACA、アクションプランの合意 - ISACA、監査結果の事実の正確性 - ISACA

最新問題: 40

以下のどれを無効にすると、無線LANのセキュリティが向上しますか？
不正アクセス？

- A. MAC (メディアアクセスコントロール) アドレスフィルタリング
- B. WPA (Wi-Fi Protected Access Protocol)
- C. LEAP (軽量拡張認証プロトコル)
- D. SSID (サービスセット識別子) ブロードキャスト

Answer: (解答を表示する)

セクション: 情報資産の保護

Explanation:

SSID ブロードキャストを無効にすると、不正ユーザーがネットワークを見つけることが難しくなるため、セキュリティが向上します。

アクセスポイントの名前。MACアドレスフィルタリングを無効にするとセキュリティが低下します。MACフィルタリングの使用トラフィックを傍受して偽造する必要があるため、WLANへのアクセスがより困難になります。

MACアドレス。WPAを無効にするとセキュリティが低下します。WPAを使用すると、通信が暗号化されるためセキュリティが向上します。

LEAPを無効にするとセキュリティが低下します。LEAPを使用すると、無線トラフィックが暗号化されるため、セキュリティが向上します。

最新問題: 41

組織が保管するプライバシー関連データのセキュリティを確保するための最良の方法は、次のうちどれですか？

- A. データの所有者に情報収集の目的を通知する。
- B. データ分類スキームを公開する。
- C. 個人を特定できる情報を暗号化します。
- D. プライバシー関連データを機密情報として分類する

Answer: D ([メッセージを残す](#))

最新問題: 42

報告された監査上の問題点に対する合意済みの是正措置のフォローアップをスケジュールする適切な時期を決定する際に、IS監査担当者にとって最も適切な指針となるのは、次のうちどれでしょうか？

- A. 進捗状況の報告によると、合意された行動の実施は順調に進んでいます。
- B. 制御動作の証拠を提供するのに十分な時間が、実装後経過している。
- C. 経営陣は合意された行動を予定通りに完了しました。
- D. 規制当局は査察訪問のスケジュールを発表しました。

Answer: B ([メッセージを残す](#))

これは、報告された監査上の問題に対する合意された是正措置のフォローアップは、被監査者が是正措置を実施し、その有効性と持続性を実証するのに十分な時間が経過した後に行われるべきであるためです。フォローアップ監査は早すぎても遅すぎてもいけません、統制運用の適切なテストと検証を可能にする合理的かつ現実的な期間に基づいて行われるべきです12。

A) 進捗状況の更新は、合意された措置の実施が順調に進んでいることを示しています。これは最適な回答ではありません。なぜなら、進捗状況の更新はフォローアップ監査のタイミングを導くのに十分ではないからです。進捗状況の更新は、是正措置の状況と課題を監視し、伝達するのに役立ちますが、管理業務の決定的な証拠を提供するものではありません。フォローアップ監査は、期待や予測ではなく、実際の結果と成果に基づいて行う必要があります12。

C) 経営陣は合意された措置の実施を予定通りに完了した。は最良の回答ではありません。なぜなら、合意された措置の実施が完了しただけでは、フォローアップ監査のタイミングを決定するのに十分ではないからです。実施の完了は、被監査者が監査上の問題に対処するために必要な措置を講じたことを示すだけであり、是正措置が効果的かつ持続可能であることを保証するものではありません。フォローアップ監査は、管理実施の完了ではなく、管理業務の評価と検証に基づいて行われるべきです12。

D). Regulators have announced a timeline for an inspection visit. is not the best answer, because the regulators' inspection visit is not relevant to guide the follow-up audit timing. The regulators' inspection visit is an external factor that may or may not coincide with the internal follow-up audit schedule. The follow-up audit should be based on the internal audit plan and objectives, not on the external audit requirements or expectations12.

最新問題: 43

Data is being transferred from an application database to a data warehouse. Some fields were not picked up in the extraction process and therefore were not transferred to the data warehouse. Which of the following is the GREATEST risk associated with this situation?

- A. Management reporting could be delayed
- B. Transaction errors may occur within the application
- C. Data that was transferred to the warehouse may not be accurate
- D. Management decisions may be based on incomplete data

Answer: ([解答を表示する](#))

The greatest risk associated with this situation is that management decisions may be based on incomplete data. If important fields are missing during the data transfer, the data in the warehouse could be inaccurate or incomplete, leading to poor decision-making based on unreliable information. This could have significant operational and strategic impacts on the organization.

最新問題: 44

Which of the following is the GREATEST benefit to an organization as a result of effective IS audit risk assessments?

- A. The scope for future audits is established
- B. Credibility with management is enhanced
- C. Low-risk areas can be eliminated
- D. Audits will be targeted to high-risk areas

Answer: ([解答を表示する](#))

最新問題: 45

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- A. nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- B. access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
- C. card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- D. the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation/Reference:

Explanation:

Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequate to trust unknown external people by allowing them to write down their alleged name without proof, e.g., identity card, driver's license. Choice B is not a concern because if the name and address of the organization was written on the card, a malicious finder could use the card to enter the organization's premises. Separating card issuance from technical rights management is a method to ensure a proper segregation of duties so that no single person can produce a functioning card for a restricted area within the organization's premises. Choices B and C are good practices, not concerns.

Choice D may be a concern, but not as important since a system failure of the card programming device would normally not mean that the readers do not function anymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

最新問題: 46

Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

- A. Degaussing
- B. Overwrite every sector of magnetic media with pattern of 1's and 0's
- C. Format magnetic media
- D. Delete File allocation table

Answer: B ([メッセージを残す](#))

Explanation/Reference:

Software tools can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media.

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed. Simply deleting files or formatting media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides.

Specialized hardware devices known as degausses can be used to erase data saved to magnetic media.

The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

オブジェクトの再利用を保証するソフトウェアツールも存在します。これらのツールは、磁気メディアの各セクターをランダムまたはあらかじめ決められたビットパターンで上書きします。上書き方式は、読み取り専用の光メディアを除くすべての電子メディアに有効です。ただし、上書きソフトウェアの使用には欠点があります。磁気メディアへの通常の書き込み操作では、データが書き込まれる際にドライブのヘッドがメディア上を往復します。ヘッドの軌跡は毎回正確に同じ経路をたどるわけではありません。その結果、各パスでごくわずかなデータ残留が生じます。特殊な機器を使用すれば、上書きされたデータを読み取ることが可能です。この場合、より高い保証を得るためには、各セクターを複数回上書きする必要があります。セキュリティ担当者は、重要度の低い情報であれば1回のパスで十分かもしれませんが、機密データは複数回上書きする必要があることを念頭に置いておくべきです。上書きソフトウェアは、USBメモリなどのソリッドステートメディア内のセクターを消去するためにも使用できます。使用されなくなったソリッドステートメディアについては、焼却や安全なリサイクルなどの物理的な破壊方法を検討することをお勧めします。

機密データへの不正アクセスを防止する最後の手段は、メディアの破壊です。シュレッダー処理、焼却、粉碎、粉末化は、メディアを物理的に破壊する一般的な方法です。消磁もメディア破壊の一形態です。高出力の消磁装置は、場合によってはハードドライブのプラッタを文字通り曲げたり歪ませたりするほど強力です。シュレッダー処理と焼却は、非剛性磁気メディアに対して効果的な破壊方法です。実際、一部のシュレッダーは、光ディスクなどの剛性メディアをシュレッダー処理することができます。ディスクを機械に投入した後に残る残留物のサイズを考慮すると、これは機密情報を含まない光メディアに対して効果的な代替手段となる可能性があります。

しかし、機密情報を含むメディアの場合、残留物のサイズが大きすぎる可能性があります。代わりに、リジッドメディアやソリッドステートメディアには、研削や粉碎が適切な選択肢となります。光メディアの表面を研削するための専用装置があり、表面を十分に傷つけて読み取り不能にするか、ディスクのデータ層を実際に削り取ります。ドライブを回収し、依頼に応じて現場で破壊し、完了証明書を発行するサービスもいくつか存在します。メディアの洗浄と廃棄に関して、最も適切なソリューションを選択、維持、支援するのは、セキュリティ専門家の責任となります。

以下の回答は誤りです。

消磁とは、磁気媒体の周囲に磁場をかけることでデータを消去する方法です。消磁装置を用いてデータを消去しますが、消磁によって磁気媒体が使用不能になる場合もあります。そのため、磁気媒体を再利用する必要がある場合は、消磁は推奨されません。Format magnetic media - Formatting magnetic media does not erase all data. Data can be recoverable after formatting using software tools.

Delete File allocation table-It will not erase all data. Data can be recoverable using software tools.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 338

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 47

オンライン注文の完全性を確保するために、次のうちどれが最も適切な管理策ですか？

- A. データ暗号化規格 (DES)
- B. デジタル署名
- C. 公開鍵暗号
- D. 多要素認証

Answer: B (メッセージを残す)

デジタル署名は、送信者から送信されたデータの真正性と完全性を検証する手段を提供するため、オンライン注文の完全性を確保する上で最も適切な制御手段です。デジタル署名は、データに暗号化アルゴリズムを適用し、その結果をデータに添付することによって作成されます。受信者は、送信者の公開鍵を使用して、データが送信中に改ざんされていないことを検証できます。また、デジタル署名は否認防止機能も提供するため、送信者はデータの送信を否定することができません。

データ暗号化規格 (DES) は、オンライン注文の機密性は確保できるものの、データの完全性は保証できない対称暗号化アルゴリズムです。DESはデータの暗号化と復号に同じ鍵を使用するため、鍵を持っている人は誰でも検出されることなくデータを改ざんできてしまいます。

公開鍵暗号方式は、オンライン注文の機密性を確保できる非対称暗号化アルゴリズムですが、データの完全性は保証できません。公開鍵暗号方式では、公開鍵と秘密鍵のペアを使用します。送信者は受信者の公開鍵でデータを暗号化し、受信者は自身の秘密鍵で復号します。

しかし、公開鍵暗号方式では、暗号化されたデータを改ざんすることを防ぐことはできません。

多要素認証は、オンライン注文の認証と認可を可能にする制御手段ですが、データの完全性を保証するものではありません。多要素認証では、ユーザーはパスワード、トークン、生体認証要素など、本人確認のための2つ以上の証拠を提示する必要があります。

多要素認証はオンライン注文への不正アクセスを防ぐことができますが、送信後のデータの改ざんを防ぐことはできません。

参考文献：

ISACA、CISA レビューマニュアル、第 27 版、2019 年、p. 281 1

ISACA、CISA試験対策問題集（解答解説付き）データベース - 12ヶ月購読プラン 2

最新問題: 48

An organization has established hiring policies and procedures designed specifically to ensure network administrators are well qualified Which type of control is in place?

- A. Detective
- B. Compensating
- C. Corrective
- D. Directive

Answer: ([解答を表示する](#))

Explanation

The type of control that is in place when an organization has established hiring policies and procedures designed specifically to ensure network administrators are well qualified is directive. Directive controls are those that guide or direct the actions of individuals or groups to achieve a desired outcome. Directive controls can also help to prevent or reduce the occurrence of undesirable events. Hiring policies and procedures are examples of directive controls that aim to ensure that only qualified and competent personnel are employed to perform IT-related tasks. References:

CISA Review Manual (Digital Version), Chapter 4, Section 4.11

CISA Online Review Course, Domain 1, Module 2, Lesson 12

最新問題: 49

非対称暗号化を用いて機密性を確保するため、メッセージは次のうちどれで暗号化されますか？

- A. 送信者の公開鍵
- B. 送信者の秘密鍵
- C. 受信者の公開鍵
- D. 受信者の秘密鍵

Answer: ([解答を表示する](#))

最新問題: 50

システム開発プロジェクトの全体的な方向性、費用、およびスケジュールについて責任を負うのは誰ですか？

- A. プロジェクトのスポンサー
- B. プロジェクト運営委員会
- C. 上級管理職
- D. プロジェクトチームリーダー

Answer: B ([メッセージを残す](#))

説明／参考資料：

プロジェクト運営委員会は、システム開発プロジェクトの全体的な方向性、費用、およびスケジュールについて責任を負う。

最新問題: 51

オフサイトのデータストレージは、時間制約のあるデータの復旧準備を行う際に同期を保つ必要があります。

それは、次のうちどれに起因するものか？

- A. 財務報告
- B. 売上報告
- C. 在庫報告
- D. トランザクション処理

Answer: D ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

時間的制約のあるデータの復旧に備える際には、オフサイトのデータストレージを同期させておく必要がある。

例えば、取引処理の結果として生じるものなど。

最新問題: 52

事業影響評価フェーズにおいて、以下のうちどれが最も重要ですか？

事業継続計画？

- A. エンドユーザーの関与
- B. 上級管理職の関与
- C. セキュリティ管理の関与
- D. IS監査への関与

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

事業継続計画における事業影響評価段階では、エンドユーザーの関与が極めて重要である。

計画。

最新問題: 53

Which of the following is the MOST efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care?

- A. Infrastructure as a Service (IaaS) provider
- B. Network segmentation

- C. Dynamic localization
- D. Software as a Service (SaaS) provider

Answer: ([解答を表示する](#))

最新問題: 54

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

- A. A monitored double-doorway entry system
- B. A monitored turnstile entry system
- C. A monitored doorway entry system
- D. A one-way door that does not allow exit after entry

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used as a deterrent control for the vulnerability of piggybacking.

最新問題: 55

What would be an IS auditor's BEST recommendation upon finding that a third-party IT service provider hosts the organization's human resources (HR) system in a foreign country?

- A. Perform background verification checks.
- B. Review third-party audit reports.
- C. Implement change management review.
- D. Conduct a privacy impact analysis.

Answer: D ([メッセージを残す](#))

The best recommendation for an IS auditor when finding that a third-party IT service provider hosts the organization's HR system in a foreign country is to conduct a privacy impact analysis. A privacy impact analysis is a systematic process that identifies and evaluates the potential risks and impacts of collecting, using, disclosing, and storing personal information. A privacy impact analysis will help the IS auditor to assess the legal, regulatory, contractual, and ethical obligations of the organization and the service provider regarding the protection of personal information. A privacy impact analysis will also help to identify and mitigate any privacy risks and gaps in the service level agreement. References:

* CISA Certification | Certified Information Systems Auditor | ISACA

* CISA Questions, Answers & Explanations Database

最新問題: 56

組織の情報分類プロセスにおけるIS監査人の主な役割は次のうちどれですか？

- A. 資産が割り当てられた分類に従って保護されていることを検証する
- B. 組織内の情報資産の分類レベルを定義する
- C. 割り当てられた分類に従って情報資産を保護する
- D. 分類レベルが規制ガイドラインに準拠していることを確認する

Answer: ([解答を表示する](#))

最新問題: 57

IS監査担当者は、組織の新しいモバイルデバイスプログラムの計画をレビューし、関連するリスクを特定するよう依頼されました。以下の推奨事項のうち、プログラムに関連するリスクを最も効果的に軽減できるのはどれですか？

- A. モバイルデバイスのセキュリティ意識向上トレーニングを開発 実施する
- B. 強力なパスワード管理を要求
- C. すべてのモバイルデバイスを業界のベストプラクティスに従って構成する
- D. モバイルデバイスのセキュリティポリシーを確立し、実施する。

Answer: ([解答を表示する](#))

最新問題: 58

アプリケーションのグラフィカルユーザーインターフェースの設計には、第4世代言語 (4GL) が最も適しています。インターフェース (GUI)。これらは、集中的なデータ計算手順の設計には不向きです。真または間違い？

- A. 真
- B. 偽

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

アプリケーションのグラフィカルユーザーインターフェースの設計には、第4世代言語 (4GL) が最も適しています。インターフェース (GUI)。これらは、高度なデータ計算処理の設計には不向きです。

最新問題: 59

組織の内部情報システム監査機能の主な目的は何ですか？

- A. 組織が適用される法律および規制要件を遵守していることを独立して証明する。
- B. 組織のリスク管理と内部統制の有効性について経営陣に保証を提供する。
- C. 持続的な改善を確実にするために、管理環境における必要な変更を特定し、開始する。
- D. 組織の方針と手順を業界のベストプラクティスと基準に照らし合わせて見直す。

Answer: A ([メッセージを残す](#))

最新問題: 60

無線通信において、受信側のデバイスが受信した通信が伝送中に改ざんされていないことを検証できるようにする制御機能はどれですか？

- A. デバイス認証とデータ発信元認証
- B. 無線侵入検知システム (IDS) および侵入防止システム (IPS)
- C. 暗号学的ハッシュの使用
- D. パケットヘッダーとトレーラー

Answer: C ([メッセージを残す](#))

Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks.

Device authentication and data origin authentication is not the correct answer since authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading. Wireless IDS / IPSs is not the correct answer since wireless IDS/IPSs have the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Packet headers and trailers alone do not ensure that the content has not been altered.

最新問題: 61

統合テスト施設 (ITF)を使用する場合、IS監査担当者は以下の点を確認する必要があります。

- A. テストには生産データが使用されます。
- B. テストデータは本番データから分離されています。
- C. テストデータジェネレーターが使用されます。
- D. マスターファイルがテストデータで更新されます。

Answer: B ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

統合テスト機能 (ITF)は、データベース内に仮想ファイルを作成し、テストトランザクションを本番データと同時に処理できるようにします。これにより、定期テストに別途テストプロセスを用意する必要がなくなりますが、テストデータを本番データから分離する必要があります。IS監査担当者は、本番データやテストデータ生成ツールを使用する必要はありません。本番マスターファイルは、テストデータで更新してはなりません。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 62

レガシーシステムを置き換える新しいアプリケーションシステムへの移行データの正確性と完全性を検証する場合、IS監査担当者がレビューするのが最も効果的です。

- A. 監査証跡
- B. ロールバック計画
- C. 持続的な結果を受け入れる
- D. データ分析結果。

Answer: A ([メッセージを残す](#))

最新問題: 63

情報セキュリティガバナンスの結果として、戦略的な整合性により以下のことが可能になります。

- A. 企業要件に基づくセキュリティ要件。
- B. ベストプラクティスに準拠した基本セキュリティ。
- C. 制度化され、商品化されたソリューション。

D. リスクへの曝露についての理解。

Answer: ([解答を表示する](#))

セクション：情報資産の保護

Explanation:

情報セキュリティガバナンスは、適切に実施されれば、以下の4つの基本的な成果をもたらすはずです。

戦略的整合性、価値提供、リスク管理、および業績測定。戦略的整合性

エンタープライズ要件に基づいてセキュリティ要件への入力を提供します。価値提供は、

標準的なセキュリティ対策、つまりベストプラクティスまたは制度化されたセキュリティとベースラインセキュリティ

汎用的なソリューション。リスク管理は、リスクへの曝露状況を理解するのに役立ちます。

最新問題: 64

Which of the following ensures confidentiality of information sent over the internet?

A. Digital signature

B. Digital certificate

C. Online Certificate Status Protocol

D. Private key cryptosystem

Answer: D ([メッセージを残す](#))

Confidentiality is assured by a private key cryptosystem. Digital signatures assure data integrity, authentication and nonrepudiation , but not confidentiality. A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity; therefore, it does not address confidentiality. Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate.

最新問題: 65

Of the following, who should authorize a project management team's request to take a mission-critical application offline to implement a new release and configuration?

A. Chief information security officer (CISO)

B. Project manager

C. Application administrator

D. Business process owner

Answer: D ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 66

ソフトウェアリリースのベースライン記録を支援するために、IS監査担当者は以下のどのプロセスを推奨すべきでしょうか？

A. 変更管理

B. バックアップとリカバリ

C. インシデント管理

D. 構成管理

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

構成管理プロセスには、ソフトウェアリリースベースラインを自動的に記録する自動化ツールが含まれる場合があります。新しいリリースが失敗した場合、ベースラインは復旧のための基準点となります。その他の選択肢は、ソフトウェアリリースベースラインを確立するために必要なプロセスを提供しておらず、ソフトウェアリリースベースラインとは関連していません。

最新問題: 67

アプリケーションの設計に深く関わったIS監査担当者が、そのアプリケーションのレビューを依頼された。監査担当者は以下のことを行うべきである。

- A. 利益相反を避けるため、依頼を辞退する。
- B. アプリケーションの知識を活用して監査を実施する。
- C. 監査管理部門に以前の関与について通知する。
- D. 監査の範囲を変更する。

Answer: C ([メッセージを残す](#))

IS監査人は、アプリケーション設計への以前の関与について監査管理部門に通知する必要があります。これは、監査の客観性や独立性に影響を与える可能性のある利益相反や偏見がないことを確認するためです。監査管理部門は、別の監査人を任命するか、適切な安全策を講じた上で同じ監査人に依頼するかを決定できます。他の選択肢は、この状況においてIS監査人が行うべきではありません。利益相反を避けるために監査の依頼を拒否することは極端な措置であり、特に他に資格のある監査人がいない場合は、必要または実行可能ではない可能性があります。アプリケーションに関する知識を用いて監査を実施することは、アプリケーションにおける潜在的な問題やエラーを見落としたり無視したりする可能性があるため、リスクを伴います。監査の範囲を変更することは、監査の質や完全性を損なう可能性があるため、推奨されません。参考文献 :CISAレビューマニュアル (デジタル版)、第2章、セクション2.1

最新問題: 68

不適切なパスワードの選択や、保護されていない通信回線での送信は、以下のような例です。

- A. 脆弱性。
- B. 脅威。
- C. 確率。
- D. 影響。

Answer: (解答を表示する)

セクション：情報資産の保護

Explanation:

脆弱性とは、脅威によって悪用される可能性のある情報リソースの特性を表します。

情報資源に損害を与える可能性のある状況または事象。確率

は脅威の発生確率を表し、影響は結果または結果を表す。

脆弱性を悪用する脅威。

最新問題: 69

許可されていない変更が本番環境に反映されるのを防ぐための最も効果的な方法はどれですか？

- A. 変更チケットを定期的にレビューし、すべての変更ドキュメントが添付されていることを確認します。
- B. 開発者と移行担当者間で職務分担を徹底する。

- C. テスト環境における変更点について徹底的なテストを実施する。
- D. 適切な業務プロセスオーナーによる変更の承認を必須とする。

Answer: ([解答を表示する](#))

セクション：情報資産の保護

最新問題: 70

Several unattended laptops containing sensitive customer data were stolen from personnel offices Which of the following would be an IS auditor's BEST recommendation to protect data in case of recurrence?

- A. Encrypt the disk drive.
- B. Require two-factor authentication
- C. Enhance physical security
- D. Require the use of cable locks

Answer: ([解答を表示する](#))

According to the CISA - Certified Information Systems Auditor Study Guide¹, the correct answer to your question is A. Encrypt the disk drive. This is because encryption is a logical security measure that can protect data even if the physical device is stolen or lost. Encryption makes the data unreadable and inaccessible without the proper key or password. The other options are not as effective as encryption in this scenario.

Two-factor authentication is a user authentication method that requires two pieces of evidence to verify the user's identity, such as a password and a code sent to a phone. However, this does not prevent unauthorized access to the data if the laptop is already logged in or if the attacker can bypass the authentication. Enhancing physical security is a preventive measure that can reduce the risk of theft, but it does not guarantee that theft will not occur or that the data will be safe if it does. Requiring the use of cable locks is another preventive measure that can deter thieves, but it can also be easily cut or removed by a determined attacker.

最新問題: 71

重大な影響を及ぼすアプリケーションの買収については、IS監査チームの参加を推奨すべきです。

- A. デューデリジェンスの初期段階。
- B. テスト段階。
- C. 最終承認段階。
- D. 予算編成段階。
- E. 選択肢のどれもでない。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

ITに大きな影響を与える買収案件においては、監査方針に定められているように、デューデリジェンスの初期段階においてIS監査の参加が必要となる場合が多い。

最新問題: 72

ベンチマークプロセスにおいて、ベンチマークパートナーはいつ特定されるのでしょうか？

- A. 設計段階で

- B. テスト段階
- C. 研究段階
- D. 開発段階

Answer: [\(解答を表示する\)](#)

説明／参考資料：

ベンチマークパートナーは、ベンチマークプロセスの調査段階で特定されます。

最新問題: 73

オンライン取引処理システムでは、取引が完全に完了するか、まったく完了しないかのどちらかであることを保証することで、データの整合性が維持されます。このデータ整合性の原則は、次のように呼ばれます。

- A. 隔離。
- B. 一貫性。
- C. 原子性。
- D. 耐久性。

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

原子性の原則は、トランザクションが完全に完了するか、まったく完了しないかのどちらかであることを要求します。エラーや中断が発生した場合、それまでに行われたすべての変更は取り消されます。一貫性は、各トランザクションにおいてデータベース内のすべての整合性条件が維持されることを保証します。分離性は、各トランザクションが他のトランザクションから分離されることを保証します。したがって、各トランザクションは、一貫性のあるデータベース状態の一部であるデータのみにアクセスします。永続性は、トランザクションが完了したとユーザーに報告された後、データベースへの変更がその後のハードウェアまたはソフトウェアの障害にも耐えることを保証します。

最新問題: 74

Which of the following is false concerning a control self-assessment?

- A. Empowers the user to take ownership and accountability
- B. Eliminates the need for a traditional audit
- C. May be used to identify high-risk areas for later review
- D. Will not have the level of independence provided by an external auditor

Answer: B ([メッセージを残す](#))

All of the statements are true except B.

A CSA is not a substitute for a traditional audit.

最新問題: 75

IS監査担当者は、最近本番環境に昇格したオンライン販売システムについて、すべてのセキュリティテストが完了していないことに気づきました。監査担当者が取るべき最善の行動は次のうちどれでしょうか？

- A. 事業へのエクスポージャーを判断する。
- B. セキュリティインシデントの監視を強化する。
- C. 第三者にセキュリティテストを実施してもらう。

D. 今後の試験活動をそれに応じて調整する。

Answer: B ([メッセージを残す](#))

最新問題: 76

組織のITシステムを保護する際、ネットワークファイアウォールが侵害された後に通常次の防御線となるのは次のうちどれですか？

- A. パーソナルファイアウォール
- B. ウイルス対策プログラム
- C. 侵入検知システム (IDS)
- D. 仮想ローカルエリアネットワーク (VLAN) の設定

Answer: ([解答を表示する](#)**)**

侵入検知システム (IDS) は、ファイアウォールの次の防衛線となります。ネットワークやサーバーのアクティビティにおける異常を検知し、犯人を特定しようとします。アンチウイルスプログラム、パーソナルファイアウォール、VLAN の設定は、さらに後の防衛線となります。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF** 問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 77

データ漏洩防止 (DLP) ソリューションにより、複数の従業員が会社のポリシーに違反して機密性の高い会社データを個人のメールアドレスに送信していることが特定されました。情報セキュリティマネージャーはまず、以下の対応を取るべきです。

- A. 法令違反の全容を把握するための調査を開始する
- B. 従業員が規定に違反していることを上級管理職に報告する
- C. 関係する従業員のインターネットアクセスを制限する
- D. 関係する従業員に連絡を取り、セキュリティ意識向上トレーニングを再受講させる。

Answer: A ([メッセージを残す](#))

セクション: 情報資産の保護

最新問題: 78

24時間365日稼働する処理環境において、データベースにはパスワードの有効期限が無期限に設定された複数の特権アプリケーションアカウントが含まれています。ビジネスへの影響を最小限に抑えつつ、このリスクに最も適切に対処できる推奨事項は次のうちどれでしょうか？

- A. アプリケーションを修正して、データベースへの直接アクセスを必要としないようにします。
- B. データベースアクセス監視を環境に導入する
- C. アプリケーションアカウントを許可するようにアクセス管理ポリシーを変更します。
- D. パスワード変更を実施するために、システム停止時間をスケジュールしてください。

Answer: B ([メッセージを残す](#))

説明

24時間365日稼働する処理環境において、パスワードの有効期限が設定されていない特権アプリケーションアカウントのリスクに対処するための最善策は、データベースアクセス監視を環境に導入することです。

データベースアクセス監視は、データベース上で実行されるすべてのアクティビティとトランザクション、特に特権ユーザーまたはアカウントによるアクティビティとトランザクションを追跡および記録するセキュリティ制御です。データベースアクセス監視は、データベースへの不正アクセスや異常なアクセス、またはアクションを検出して警告することで、パスワードの有効期限が無期限に設定されている特権アプリケーションアカウントのリスクに対処するのに役立ちます。他のオプションは、業務の中断やアクセス管理ポリシーへの違反を引き起こす可能性があるため、データベースアクセス監視ほどリスクに対処するのに効果的ではありません。アプリケーションを変更してデータベースへの直接アクセスを必要としないようにすることは、複雑でコストのかかるソリューションであり、アプリケーションの機能やパフォーマンスに影響を与える可能性があり、24時間365日稼働する処理環境では実現不可能または実用的ではない可能性があります。アプリケーションアカウントを許可するようにアクセス管理ポリシーを変更することは、ポリシーに例外や抜け穴が生じる可能性があり、パスワード管理のベストプラクティスや標準に準拠しない可能性があるため、リスクの高いソリューションです。パスワード変更を実施するためにダウンタイムをスケジュールすることは、システムまたはアプリケーションの可用性や継続性に影響を与える可能性のある中断を伴うソリューションであり、24時間365日稼働する処理環境では受け入れられない、または不可能な場合があります。

参考文献 :CISAレビューマニュアル (デジタル版)、第5章、セクション5.2.4

最新問題: 79

組織のリスク管理慣行の監査中に、IS監査担当者は、文書化された複数のITリスク承認が、割り当てられた有効期限後に適時に更新されていないことを発見しました。この発見を評価する際に、関連する影響を最も大幅に軽減する緩和要因はどれですか？

- A. 業務プロセスに対する補償的な統制が文書化されています。
- B. リスク受容は、適切な上級管理職によって事前に審査され、承認されています。
- C. リスク受容が承認されて以来、事業環境に大きな変化はありません。
- D. 問題のあるリスク受容は、全体の人口のごく一部を反映している。

Answer: A ([メッセージを残す](#))

ITリスクの承認を適時に更新しないことによる影響を最も効果的に軽減する要因は、業務プロセスに対する文書化された代替統制を設けることです。代替統制とは、主要な統制が実行不可能または費用対効果が低い場合に、リスクを軽減または排除する代替統制のことです。上級管理職による事前の承認、変化のない業務環境、問題発生率の低さといった他の要因は、代替統制ほど効果的にリスクを軽減しません。参考文献 :ISACA CISAレビューマニュアル第27版第1章

最新問題: 80

EDI環境における主なセキュリティ上の懸念事項は何ですか？

- A. トランザクション認証
- B. トランザクションの完全性
- C. 取引の正確性
- D. 取引承認

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:EDI環境において、トランザクションの認証は主要なセキュリティ上の懸念事項です。

最新問題: 81

並行テストを実施する主な目的は次のうちどれですか？

- A. システムが費用対効果が高いかどうかを判断する
- B. 包括的なユニットおよびシステムテストを可能にする
- C. プログラムインターフェース内のエラーをファイルで強調表示する
- D. 新システムがユーザーの要求を満たすことを保証する

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

並行テストの目的は、新しいシステムの実装がユーザーの要求を満たすことを確認することです。並行テストの結果、実際には旧システムの方が新システムよりも優れていることが判明する場合がありますが、それが主な理由ではありません。並行テストの前に、単体テストとシステムテストが完了します。システムテストでは、プログラムとファイルのインターフェースにおけるエラーがテストされます。

最新問題: 82

次の攻撃タイプのうち、C言語のprint()関数のフォーマット文字列パラメータとして、フィルタリングされていないユーザー入力を使用するものはどれですか？

- A. バッファオーバーフロー
- B. フォーマット文字列の脆弱性
- C. 整数オーバーフロー
- D. コードインジェクション
- E. コマンドインジェクション
- F. 選択肢に該当しない。

Answer: ([解答を表示する](#)**)**

説明／参考資料：

Explanation:

フォーマット文字列攻撃は、最近発見された新しいタイプの脆弱性です。この攻撃は、プログラムをクラッシュさせたり、悪意のあるコードを実行したりするために悪用される可能性があります。この問題は、print() などのフォーマット処理を行う特定の C 関数において、フィルタリングされていないユーザー入力をフォーマット文字列パラメータとして使用していることに起因します。悪意のあるユーザーは、%s や %x などのフォーマットトークンを使用して、スタックやメモリ内の他の場所からデータを出力する可能性があります。また、%n フォーマットトークンを使用して、任意の場所に任意のデータを書き込むことも可能です。

最新問題: 83

Which of the following is the BEST security control to validate the integrity of data communicated between production databases and a big data analytics system?

- A. Running and comparing the count function within the in-scope data sets
- B. Encrypting in-scope data sets
- C. Hashing in-scope data sets
- D. Hosting a digital certificate for in-scope data sets

Answer: C ([メッセージを残す](#))

最新問題: 84

データ処理施設に設置された煙感知器の有効性にとって、次のうちどれが最も重要ですか？

- A. 検出器は作動時に可聴アラームを発します。
- B. 検出器は乾式配管消火システムに接続されています。
- C. 検出器は湿式配管消火システムに接続されています。
- D. 検出器は適切な業界認証を取得しています。

Answer: A ([メッセージを残す](#))

最新問題: 85

An IS auditor is providing input to an RFP to acquire a financial application system. Which of the following is MOST important for the auditor to recommend?

- A. The application should meet the organization's requirements.
- B. Audit trails should be included in the design.
- C. Potential suppliers should have experience in the relevant area.
- D. Vendor employee background checks should be conducted regularly.

Answer: ([解答を表示する](#)**)**

This is because audit trails are records of system activity and user actions that can provide evidence of the validity and integrity of transactions and data in a financial application system. Audit trails can help to ensure compliance with laws, regulations, policies, and standards, as well as to detect and prevent fraud, errors, or misuse of information. Audit trails can also facilitate auditing, monitoring, and evaluation of the financial application system's performance and controls¹.

The application should meet the organization's requirements (A) is not the best answer, because it is a general and obvious criterion that applies to any application system acquisition, not a specific and important recommendation for a financial application system. The organization's requirements should be clearly defined and documented in the RFP, but they may not necessarily include audit trails as a design feature.

Potential suppliers should have experience in the relevant area © is not the best answer, because it is a factor that affects the selection of the supplier, not the design of the financial application system. The experience and reputation of potential suppliers should be evaluated and verified during the RFP process, but they may not guarantee that the supplier will include audit trails in the design.

ベンダー従業員の身元調査を定期的実施する D)は、ベンダーのセキュリティと信頼性に影響を与える措置であり、財務アプリケーションシステムの設計には影響しないため、最適な回答ではありません。ベンダー従業員の身元調査は、ベンダー管理およびデューデリジェンスプロセスの一環として実施されるべきですが、ベンダーが設計に監査証跡を含めることを保証するものではありません。

最新問題: 86

What can be implemented to provide the highest level of protection from external attack?

- A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- B. Configuring the firewall as a screened host behind a router

- C. Configuring the firewall as the protecting bastion host
- D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

最新問題: 87

Wi-Fi Protected Accessは、どのIEEE規格の大部分を実装していますか？

- A. 802.11i
- B. 802.11g
- C. 802.11x
- D. 802.11v
- E. 選択肢のどれもでない。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

最新問題: 88

新しいアプリケーションシステムの導入を監査する際に、IS監査担当者に最も確実な保証を与えるのは次のうちどれでしょうか？

- A. 統計的サンプリング
- B. 属性サンプリング
- C. システム所有者による承認
- D. 実体試験

Answer: ([解答を表示する](#))

最新問題: 89

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

- A. Power line conditioners
- B. Surge protective devices
- C. Alternative power supplies
- D. Interruptible power supplies

Answer: ([解答を表示する](#))

Power line conditioners are used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine. Any valleys are removed by power stored in the equipment. Surge protection devices protect against high-voltage bursts. Alternative power supplies are intended for computer equipment running for longer periods and are normally coupled with other devices such as an uninterruptible power supply (UPS) to compensate for the power loss until the alternate power supply becomes available. An interruptible power supply would cause the equipment to come down whenever there was a power failure.

最新問題: 90

Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

- A.** Presentation layer
- B.** Desktop Access Layer
- C.** Data Mart layer
- D.** Data access layer

Answer: C ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components The enterprise data flow architecture (EDFA) A logical data architecture Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer - This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced score cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data - Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data - Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data - Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse - This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A properly constituted DW should support three basic form of an inquiry.

Drilling up and drilling down - Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across - Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis - The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer - This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer - This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer - This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to pre-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer - The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer - This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer - This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram - De-construct business processes.

エンティティ関係図 - データエンティティとその関係性を図示します。これらのデータ分析手法は、エンタープライズデータモデルの開発において重要な役割を果たします。しかし、知識豊富なビジネス担当者がプロセスに関与することも不可欠です。これにより、データのビジネス目的とコンテキストを適切に理解することができます。また、既存のシステムやデータベースから最適とは言えないデータ構成がデータウェアハウスに複製されるリスクも軽減されます。

以下の回答は誤りでした。

デスクトップアクセス層、またはプレゼンテーション層とは、エンドユーザーが情報を直接扱う層です。この層には、スプレッドシート、直接クエリツール、CongasやBusiness Objectsなどのベンダーが提供するレポート作成・分析スイートといった使い慣れたデスクトップツール、バランスソースカードやデジタルダッシュボードなどの専用アプリケーションが含まれます。

データアクセス層 - この層は、データストレージ層とデータ品質層をデータソース層のデータストアに接続する役割を果たし、その過程で、これらのデータストアがどのように構成されているかを正確に知る必要性をなくします。現在の技術では、リレーショナルデータベースに格納されていないデータであっても、SQLを使用してデータにアクセスできます。

参照：

最新問題: 91

ITフォレンジック監査の主な目的は以下のとおりです。

- A. 企業不正に関する調査に参加する。
- B. システム異常発生後の証拠の体系的な収集。
- C. 組織の財務諸表の正確性を評価する
- D. 犯罪行為があったと判断するため。

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

選択肢Bは、フォレンジック監査について説明しています。収集された証拠は、その後、司法手続きで使用される可能性があります。

フォレンジック監査は、企業不正に限定されるものではありません。組織の財務諸表の正確性を評価することは、フォレンジック監査の目的ではありません。犯罪行為の結論を出すことは、法的手続きの一部であり、フォレンジック監査の目的ではありません。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfumps**)

最新問題: 92

A new system development project is running late against a critical implementation deadline.

Which of the following is the MOST important activity?

- A. Perform a pre-implementation audit.
- B. Ensure that code has been reviewed.
- C. Perform user acceptance testing (UAT).
- D. Document last-minute enhancements.

Answer: ([解答を表示する](#))

最新問題: 93

法医学的データ収集および保存手順において、最も重要な項目は次のうちどれですか？

- A. デバイスの物理的セキュリティを確保する
- B. データの整合性の維持
- C. 保管管理の連鎖を維持する
- D. 使用するツールの決定

Answer: B ([メッセージを残す](#))

フォレンジックデータ収集および保存手順において最も重要なことは、データの完全性を維持することです。データの完全性とは、データがライフサイクル全体を通して正確、完全、かつ一貫していることを保証する特性です。データの完全性を維持することは、フォレンジックデータ収集および保存手順において不可欠です。なぜなら、データの完全性を維持することで、データが法的手続きや調査において有効かつ信頼できる証拠として使用できることが保証されるからです。データの完全性を維持するには、ハッシュ、チェックサム、デジタル署名、書き込みブロッカー、改ざん防止シール、タイムスタンプなどの方法を用いることができます。他の方法は、データの有効性や信頼性に影響を与えないため、フォレンジックデータ収集および保存手順においてデータの完全性を維持することほど重要ではありません。デバイスの物理的なセキュリティを確保することは、デバイスを不正アクセス、盗難、損傷、破壊から保護するセキュリティ対策ですが、デバイス上のデータが正確、完全、かつ一貫していることを保証するものではありません。証拠保全の連鎖を維持することは、フォレンジック活動に関与する様々な関係者間でのデバイスやデータの取り扱いと移転を記録・追跡する文書化手法ですが、デバイス上のデータが正確、完全、かつ一貫していることを保証するものではありません。使用するツールを決定することは、フォレンジックデータの収集と保存手順に適したツールを選択して準備する計画活動ですが、ツールによって収集・保存されたデータが正確、完全、かつ一貫していることを保証するものではありません。参考文献：CISAレビューマニュアル（デジタル版）、第5章、セクション5.4

最新問題: 94

サービス品質（QoS）の利点は、以下の点です。

- A. ネットワーク全体の可用性とパフォーマンスが大幅に向上します。
- B. 通信事業者は、正確なサービスレベル遵守レポートを会社に提供する。
- C. 参加アプリケーションには、サービスレベルが保証されます。
- D. 通信リンクは、安全なオンライン取引を実行するためのセキュリティ制御によってサポートされます。

Answer: C ([メッセージを残す](#))

QoSの主な機能は、特定のトラフィックに帯域幅の専用部分を割り当てることで、ビジネスアプリケーションとエンドユーザーに優先順位を付け、ネットワークパフォーマンスを最適化することです。選択肢Aは正しくありません。なぜなら、通信自体が改善されるわけではないからです。特定のアプリケーションのデータ交換速度は速くなる可能性があります、可用性は向上しません。多くの通信事業者が使用しているQoSツールはサービスレベルのレポートを提供しませんが、サービスレベルレポートを生成するツールもあります。QoSがファイアウォール、VPN、暗号化ツールなどと統合されている場合でも、ツール自体はセキュリティ制御を提供するものではありません。

最新問題: 95

Which of the following types of attack often take advantage of curiosity or greed to deliver malware?

- A. Gimmes
- B. Tripwire
- C. Icing
- D. Soft coding
- E. Pretexting
- F. None of the choices.

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Gimmes take advantage of curiosity or greed to deliver malware. Also known as a Trojan Horse, gimmes

can arrive as an email attachment promising anything. The recipient is expected to give in to the need to the program and open the attachment. In addition, many users will blindly click on any attachments they 少しでも正当に見えるものを受け取る。

最新問題: 96

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- A. Governing
- B. Culture
- C. Enabling and support
- D. Emergence

Answer: D (メッセージを残す)

Section: Governance and Management of IT

Explanation:

Emergence - which connotes surfacing, developing, growing and evolving - refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

For your exam you should know the information below.

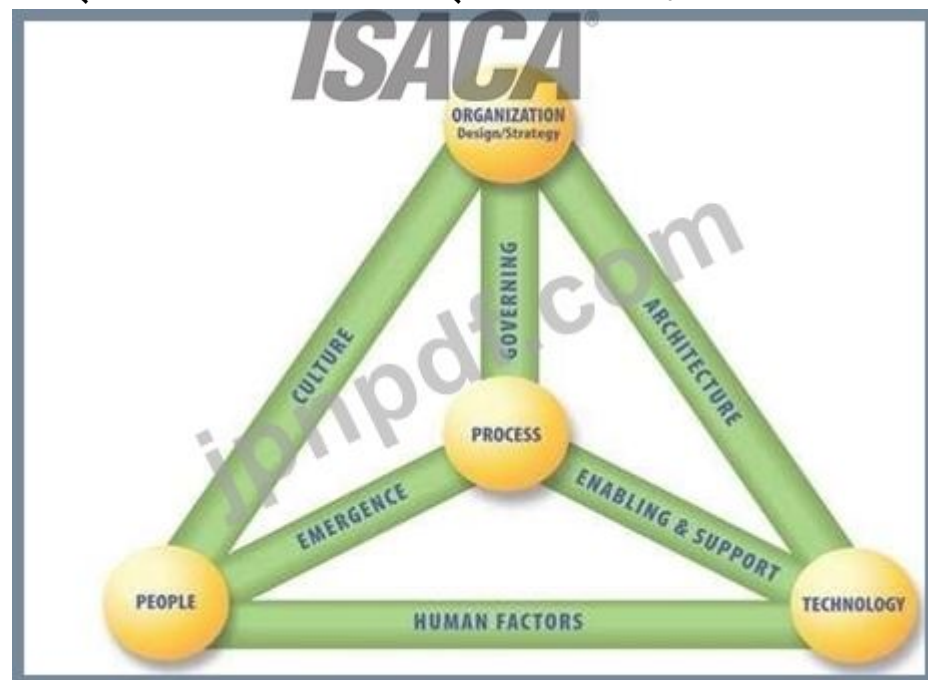
Business Model for Information Security

情報セキュリティのビジネスモデル (BMIS)は、米国南カリフォルニア大学マーシャル・ビジネススクールの重要情報インフラ保護研究所で生まれました。ISACAは、システムセキュリティ管理モデルの開発に取り組んでいます。BMISは、同研究所が開発した基礎概念に基づき、情報セキュリティ管理にビジネス指向のアプローチを採用しています。このモデルは、システム思考を活用して企業内の複雑な関係性を明確にし、セキュリティをより効果的に管理します。モデルの基盤となる要素と動的な相互接続は、情報セキュリティプログラムの境界を定め、プログラムがどのように機能し、内部および外部の変化にどのように反応するかをモデル化します。BMISは、Cubitなどのフレームワークのコンテキストを提供します。

システム理論の本質は、システムを正確に理解するためには、単に構成要素の総和としてではなく、全体として捉える必要があるという点にあります。全体論的なアプローチでは、システムを完全な機能単位として考察します。システム理論のもう一つの原則は、システムの一部を理解することで、他の部分を理解することができるという点です。「システム思考」は、システムがどのように相互作用し、複雑なシステムがどのように機能し、全体は部分の総和以上である」理由を考察することを指す、広く認知された用語です。システム理論は、多くの場合目に見えない予期せぬ方法で相互作用する、事象、関係、反応、結果、技術、プロセス、および人々の複雑なネットワークとして最も正確に説明できます。相互作用の挙動と結果を研究することで、管理者は組織システムとその機能の仕方をよりよく理解することができます。企業内のあらゆる分野の管理は、システム思考の観点からアプローチすることで強化できますが、その導入はリスク管理に確実に役立ちます。

システムアプローチが他の分野で収めてきた成功は、セキュリティ分野においても同様の効果が期待できることを示しています。近年、企業がセキュリティ問題に適切に対処できずに深刻な失敗を繰り返すのは、セキュリティを定義し、すべてのステークホルダーにとって理解しやすく関連性の高い形で提示できていないことが大きな原因です。情報セキュリティ管理にシステムア

ブローチを採用することで、情報セキュリティ管理者は複雑で動的な環境に対応できるようになり、企業内の連携、業務変更への適応、戦略的不確実性への対応、外部要因の影響への耐性といった面で有益な効果が得られます。そのモデルを以下に示します。



上記に示したように、このモデルは、6つの動的な相互接続によって連結された4つの要素から構成される、柔軟な3次元のピラミッド型構造として捉えるのが最適です。

モデルのすべての要素は相互に作用し合います。モデルのいずれかの部分が変更されたり、対処されなかったり、不適切に管理されたりすると、モデルの均衡が損なわれる可能性があります。動的な相互接続は張力として働き、企業の変化に応じて押し引きの力を発揮し、モデルが必要に応じて適応できるようにします。

このモデルを構成する4つの要素は以下のとおりです。

1. 組織設計と戦略 - 組織とは、明確に定義された役割の中で互いに相互作用し、共通の目標に向かって活動する人、資産、プロセスのネットワークである。

企業の戦略は、事業目標、達成すべき目的、追求すべき価値観や使命を明確に定めたものです。それは企業の成功の方程式であり、基本的な方向性を示します。戦略は外部要因と内部要因に適応する必要があります。戦略を策定する上で最も重要な要素はリソースであり、リソースには様々な種類（人材 設備、ノウハウなど）があります。設計とは、組織が戦略をどのように実行するかを定義するものです。プロセス、文化、そしてアーキテクチャは、設計を決定する上で重要な要素となります。

2. 人材 - 人材とその周辺のセキュリティ問題。戦略の各部分を誰が（設計を通じて）実行するかを定義します。人材は人間の集団を表し、価値観、行動、偏見を考慮に入れる必要があります。社内においては、情報セキュリティマネージャーが人事部や法務部と協力して、次のような問題に対処することが不可欠です。

採用戦略（アクセス、身元調査、面接、役割と責任）、雇用問題（オフィスの場所、ツールとデータへのアクセス、トレーニングと意識向上、社内異動）、退職（退職理由 退職時期、役割と責任、システムへのアクセス、他の従業員へのアクセス）。社外では、顧客、サプライヤー、メディア、利害関係者などが企業に強い影響力を持つ可能性があり、セキュリティ体制の中で考慮する必要があります。

3. プロセス - 物事を成し遂げるための公式および非公式のメカニズム（大小 単純および複雑）を含み、すべての動的な相互関係への重要なリンクを提供する。

プロセスは、リスク、可用性、完全性、機密性を特定、測定、管理、制御するとともに、説明責任を確保する。これらは戦略から派生し、組織要素の運用面を実行する。

企業にとって有利となるためには、プロセスは以下の条件を満たす必要がある。

ビジネス要件を満たし、ポリシーに準拠する
新たな可能性を考慮し、変化する要件に適応する
適切な人事部門に文書化して伝達する

導入後は、効率性と有効性を確保するために定期的に見直す必要がある。

4. テクノロジー — プロセスの効率化を図るためのあらゆるツール、アプリケーション、インフラストラクチャから構成される。テクノロジーは頻繁に変化する進化する要素であり、それ自体に動的なリスクが存在する。一般的な企業がテクノロジーに依存していることを考えると、テクノロジーは企業のインフラストラクチャの中核を成し、その使命を達成する上で不可欠な要素となる。

企業の経営陣は、セキュリティ上の脅威やリスクを解決する手段としてテクノロジーを捉えることが多い。技術的な対策は一部のリスクを軽減するのに役立つものの、テクノロジーを情報セキュリティの万能ソリューションとみなすべきではない。

テクノロジーは、ユーザーと組織文化によって大きく影響を受けます。テクノロジーを信用しない人もいれば、使い方を習得していない人もいます。また、テクノロジーによって作業効率が低下すると感じる人もいます。理由は何であれ、情報セキュリティ管理者は、多くの人が技術的な制御を回避しようとする可能性があることを認識しておく必要があります。

動的な相互接続

動的な相互接続は、要素同士を結びつけ、状況の変化に応じて押し引きする多方向の力を及ぼします。動的な相互接続の中で発生する動作や挙動は、モデルのバランスを崩したり、均衡状態に戻したりする可能性があります。

6つの動的な相互接続は以下のとおりです。

1. ガバナンス - ガバナンスとは、企業を統括するものであり、戦略的なリーダーシップが求められます。ガバナンスは、企業が活動する範囲を定め、業績を監視し、活動を記述し、コンプライアンスを達成すると同時に、新たな状況への適応性を提供するプロセスの中で実施されます。ガバナンスには、目標が決定され明確に定義されていること、リスクが適切に管理されていることを確認すること、そして企業の資源が責任を持って使用されていることを検証することが含まれます。

2. 文化 - 文化とは、行動、信念、前提、態度、物事のやり方のパターンです。それは創発的かつ学習されたものであり、安心感を生み出します。文化は、集団が共通の経験を重ねるにつれて、一種の共有された歴史として進化します。こうした類似した経験は特定の反応を引き起こし、それが期待される共有された行動の集合体となります。これらの行動は暗黙のルールとなり、共通の歴史を持つすべての人々が共有する規範となります。企業の文化を理解することは重要です。なぜなら、文化はどのような情報が考慮され、どのように解釈され、どのように活用されるかに深く影響を与えるからです。文化は、国家レベル（法律／規制政治、伝統）、組織レベル（方針階層構造、期待）、社会レベル（家族エチケット）など、多くのレベルで存在し得ます。文化は外部要因と内部要因の両方から形成され、組織のパターンに影響を与え、また組織のパターンによっても影響を受けます。

3. Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence - Emergence - which connotes surfacing, developing, growing and evolving - refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5. Human factors - The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.

6. Architecture - A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

ガバナンス — ガバナンスとは、企業を統括するものであり、戦略的なリーダーシップが求められます。ガバナンスは、企業が活動する範囲を定め、業績を監視し、活動を記述し、コンプライアンスを達成すると同時に、新たな状況への適応性を確保するためのプロセスの中で実施されます。

ガバナンスには、目標が決定され明確に定義されていること、リスクが適切に管理されていることを確認すること、そして企業の資源が責任を持って使用されていることを検証することが含まれる。

有効化とサポート - 有効化とサポートの動的な相互接続は、テクノロジー要素とプロセス要素を結び付けます。人々が技術的なセキュリティ対策、ポリシー、手順を遵守することを確実にする方法の1つは、プロセスを使いやすく、容易にすることです。透明性は、セキュリティが効果的な作業能力を阻害しないことをユーザーに保証することで、セキュリティ制御の受け入れを促進するのに役立ちます。テクノロジーとプロセスの両方に影響を与える多くのアクションは、有効化とサポートの動的な相互接続の中で発生します。ポリシー、標準、ガイドラインは、利益相反を軽減または排除し、変化するビジネス目標をサポートする柔軟性を維持し、人々が受け入れやすく、容易に従えるように設計する必要があります。

文化とは、行動、信念、前提、態度、物事のやり方のパターンです。それは自然に生まれ、学習されるものであり、安心感を生み出します。文化は、集団が共通の経験を重ねるにつれて、一種の共有された歴史として進化します。こうした類似した経験は特定の反応を引き起こし、それが期待される共通の行動となります。これらの行動は暗黙のルールとなり、共通の歴史を持つすべての人々が共有する規範となります。企業の文化を理解することは重要です。なぜなら、文化はどのような情報が考慮され、どのように解釈され、どのように活用されるかに深く影響を与えるからです。文化は、国家レベル（法律／規制 政治、伝統）、組織レベル（方針 階層構造、期待）、社会レベル（家族 エチケット）など、多くのレベルで存在し得ます。文化は外部要因と内部要因の両方から形成され、組織のパターンに影響を与え、また組織のパターンによっても影響を受けます。

参照：

CISAレビューマニュアル2014年版、37ページと38ページ

<http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>

最新問題: 97

Which of the following observations should be of GREATEST concern to an IS auditor reviewing a large organization's virtualization environment?

- A. Guest tools have been installed without sufficient access control,
- B. A rootkit was found on the host operating system

- C. An unused printer has been left connected to the host system.
- D. Host inspection capabilities have been disabled

Answer: B ([メッセージを残す](#))

最新問題: 98

ビジネスインパクト分析 (BIA) を実施する際に使用されるデータは、次のうちどれですか？

- A. 現在の事業が将来の事業に及ぼす影響予測
- B. 規制遵守にかかる費用
- C. 現在の事業運営に関する費用便益分析
- D. 事業回復にかかる予想費用。

Answer: A ([メッセージを残す](#))

セクション :ITのガバナンスと管理

最新問題: 99

An IS auditor is reviewing the perimeter security design of a network. Which of the following provides the GREATEST assurance outgoing Internet traffic is controlled?

- A. Intrusion detection system (IDS)
- B. Security information and event management (SIEM) system
- C. Stateful firewall
- D. Load balancer

Answer: C ([メッセージを残す](#))

A stateful firewall provides the greatest assurance that outgoing Internet traffic is controlled, as it monitors and filters packets based on their source, destination and connection state. A stateful firewall can prevent unauthorized or malicious traffic from leaving the network, as well as block incoming traffic that does not match an established connection. An intrusion detection system (IDS) can detect and alert on suspicious or anomalous traffic, but it does not block or control it. A security information and event management (SIEM) system can collect and analyze logs and events from various sources, but it does not directly control traffic. A load balancer can distribute traffic among multiple servers, but it does not filter or monitor it. References:

CISA Review Manual (Digital Version), Chapter 6, Section 6.2

最新問題: 100

Which of the following will be the MOST effective method to verify that a service vendor keeps control levels as required by the client?

- A. Conduct periodic on-site assessments using agreed-upon criteria.
- B. Periodically review the service level agreement (SLA) with the vendor.
- C. Conduct an unannounced vulnerability assessment of vendor's IT systems.
- D. Obtain evidence of the vendor's control self-assessment (CSA).

Answer: A ([メッセージを残す](#))

Explanation

The most effective method to verify that a service vendor keeps control levels as required by the client is to conduct periodic on-site assessments using agreed-upon criteria. On-site assessments can provide direct evidence of whether the vendor's controls are operating effectively and consistently in accordance with the client's expectations and requirements. Agreed-upon criteria can

ensure that the assessments are objective, relevant, and reliable. The other options are not as effective as on-site assessments in verifying the vendor's control levels. Periodically reviewing the SLA with the vendor can help monitor whether the vendor meets its contractual obligations and service standards, but it does not provide assurance of whether the vendor's controls are adequate or sufficient. Conducting an unannounced vulnerability assessment of vendor's IT systems can help identify any weaknesses or gaps in the vendor's security controls, but it may violate the terms and conditions of the vendor-client relationship or cause operational disruptions. Obtaining evidence of the vendor's CSA can provide some indication of whether the vendor's controls are self-monitored and reported, but it does not verify whether the vendor's controls are independent or accurate.

References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

最新問題: 101

IS監査担当者が組織のインシデント管理プロセスと手順をレビューしています。監査担当者が最も懸念すべき点は次のうちどれでしょうか？

- A. インシデント検出が不十分
- B. 無効な事象分類
- C. 事後検証が不十分
- D. インシデントの優先順位付けが効果的でない

Answer: A ([メッセージを残す](#))

最新問題: 102

以前合意された勧告は、被監査者が当初の調査結果に同意しなくなったため実施されませんでした。IS監査人が最初にとるべき行動は次のとおりです。

- A. 元の勧告の実施を要求する。
- B. フォローアップ監査報告書からその所見を除外する。
- C. 意見の相違を監査委員会にエスカレートする。
- D. 意見の相違の理由を評価する。

Answer: ([解答を表示する](#)**)**

最新問題: 103

生体認証システムの精度指標は次のとおりです。

- A. システム応答時間。
- B. 登録時間。
- C. 入力ファイルサイズ。
- D. 誤認率。

Answer: ([解答を表示する](#)**)**

説明／参考資料：

Explanation:

生体認証ソリューションでは、主に3つの精度指標が使用されます。それは、誤拒否率 (FRR)、交差エラー率 (CER)、誤受入率 (FAR)です。FRRは、有効な個人がどれくらいの頻度で拒否されるかを示す指標です。

FARは、無効な個人が受け入れられる頻度を示す指標です。CERは、誤拒否率と誤受入率が等しくなるタイミングを示す指標です。選択肢AとBは、パフォーマンス指標です。

最新問題: 104

レガシーシステムを置き換える新しいアプリケーションシステムへの移行データの正確性と完全性を検証する場合、IS監査担当者がレビューするのが最も効果的です。

- A. データ分析結果。
- B. 監査証跡
- C. 持続的な結果を受け入れる
- D. ロールバック計画

Answer: A ([メッセージを残す](#))

説明

レガシーシステムを置き換える新しいアプリケーションシステムの移行データの正確性と完全性を検証する場合、IS監査担当者がデータ分析の結果をレビューすることが最も効果的です。データ分析とは、ソフトウェアツールと統計的手法を用いて大量のデータを分析し、パターン、異常、エラー、または矛盾を特定する手法です。データ分析は、ソースデータセットとターゲットデータセットを比較し、データの品質と整合性を検証し、移行プロセス中のデータ損失や破損を検出するのに役立ちます。他の方法は、監査証跡がデータに対して実行された操作のみを記録し、受け入れテストの結果が新しいシステムの機能性のみを検証し、ロールバック計画が移行失敗時の緊急対策のみを提供するという点で、それほど効果的ではありません。参考文献 :CISAレビューマニュアル (デジタル版)1、第5章、セクション5.2.6

最新問題: 105

During an audit, the IS auditor finds that in many cases excessive rights were not removed from a system. Which of the following is the auditor's BEST recommendation?

- A. Line management should regularly review and request modification of access rights.
- B. System administrators should ensure consistency of assigned rights.
- C. Human resources (HR) should delete access rights of terminated employees.
- D. IT security should regularly revoke excessive system rights.

Answer: ([解答を表示する](#))

最新問題: 106

IS品質保証 QA)グループは以下の責任を負います。

- A. プログラムの変更が確立された基準に準拠していることを確認する。
- B. システム処理から受け取った出力が完全であることを確認する。
- C. コンピュータ処理タスクの実行状況の監視
- D. 偶発的なデータ漏洩からデータを保護するための手順を設計する。

Answer: A ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 107

A CIO has asked an IS auditor to implement several security controls for an organization's IT processes and systems. The auditor should:

- A. refuse due to independence issues.
- B. obtain approval from executive management for the implementation
- C. communicate the conflict of interest to audit management
- D. perform the assignment and future audits with due professional care.

Answer: A ([メッセージを残す](#))

最新問題: 108

IS部門が正式に文書化された方法論、ポリシー、および標準を使用していないことをIS監査人が発見した場合、監査人は何をすべきでしょうか？最適な回答を選択してください。

- A. IT文書の不足は、通常、IT監査でテストされる統制にとって重要ではありません。
- B. 監査人は、少なくとも非公式な基準と方針を文書化すべきである。さらに、IS監査人は、実施すべき正式な文書化された方針を作成すべきである。
- C. 監査人は、少なくとも非公式な基準や方針を文書化し、遵守状況をテストする必要があります。さらに、IS監査人は、経営陣に対し、正式な文書化された方針を策定し、実施することを推奨する必要があります。
- D. 監査人は、少なくとも非公式な基準と方針を文書化し、それに準拠しているかどうかをテストする必要があります。さらに、IS監査人は、実施すべき正式な文書化された方針を作成する必要があります。

Answer: C ([メッセージを残す](#))

IS監査担当者が、IS部門が正式に文書化された方法論、方針、および基準を使用していないことを確認した場合、少なくとも非公式な基準と方針を文書化し、遵守状況をテストする必要があります。さらに、IS監査担当者は、経営陣に対し、正式に文書化された方針を策定し、実施するよう勧告する必要があります。

最新問題: 109

中小規模の組織において、インターネット経由でプライベートネットワークを接続するための、最も安全かつ経済的な方法は次のうちどれですか？

- A. 仮想プライベートネットワーク
- B. 専用線
- C. 専用線
- D. 統合サービスデジタルネットワーク

Answer: A ([メッセージを残す](#))

最も安全な方法は、仮想プライベートネットワーク (VPN) です。VPNは暗号化、認証、トンネリングを用いて、プライベートネットワークからインターネットへデータを安全に転送します。選択肢B、C、Dは、通常、中小規模の組織にとって費用が高すぎて実用的ではないネットワーク接続オプションです。

最新問題: 110

ネットワーク活動を監視するサードパーティサービスプロバイダーのIS監査を計画する際に、最初に行うべき手順は次のうちどれですか？

- A. 第三者の監視ログとインシデント対応状況を確認する
- B. 第三者プロバイダーの役割と責任を確認する
- C. 組織の第三者監視プロセスを評価する
- D. 組織がプロバイダーと安全な接続を確立しているかどうかを確認する

Answer: B ([メッセージを残す](#))

ネットワーク活動を監視するサードパーティサービスプロバイダーのIS監査を計画する際の最初のステップは、サードパーティプロバイダーの役割と責任を確認することです。これにより、監査の範囲、目的、期待事項を明確にするとともに、組織とプロバイダー間のサービスレベル契約 (SLA) における潜在的なリスク、問題、またはギャップを特定することができます。サードパーティの監視ログとインシデント処理を確認し、組織のサードパーティ監視プロセスを評価し、組織がプロバイダーと安全な接続を確立しているかどうかを判断することは重要なステップですが、これらはプロバイダーの役割と責任を確認した後に行う必要があります。参考文献 :CISAレビューマニュアル (デジタル版) 1、269ページ。

最新問題: 111

.What are used as the framework for developing logical access controls?

- A. Information systems security policies
- B. Organizational security policies
- C. Access Control Lists (ACL)
- D. Organizational charts for identifying roles and responsibilities

Answer: A ([メッセージを残す](#))

Information systems security policies are used as the framework for developing logical access controls.

最新問題: 112

セキュリティ管理手順では、以下のものへの読み取り専用アクセスが必要です。

- A. アクセス制御テーブル。
- B. セキュリティログファイル。
- C. ログ記録オプション。
- D. ユーザープロフィール。

Answer: (解答を表示する)

セクション：情報資産の保護

Explanation:

セキュリティ管理手順では、セキュリティログファイルへの読み取り専用アクセスが必要です。これは、生成されたログが改ざんされないようにするためです。ログは証拠を提供し、疑わしい取引や活動を追跡します。セキュリティ管理手順では、アクセス制御テーブルへの書き込みアクセスが必要です。これは、承認された業務要件に従って権限を管理および更新するためです。ログオプションには書き込みアクセスが必要です。これは、管理者が取引やユーザー活動の監視、取得、保存、処理、および報告方法を更新できるようにするためです。

最新問題: 113

Which of the following is the PRIMARY benefit of using a SIEM tool to collate high amounts of data collected across various security tools?

- A. Reducing the number of false positive incidents
- B. Correlating many isolated events to create a single source of record
- C. Decreasing the effort needed to monitor security events
- D. Reducing the number of isolated events noted as incidents

Answer: B ([メッセージを残す](#))

最新問題: 114

次のアプローチのうち、データ分析を活用して新規アカウント作成プロセスのテストを促進するものはどれですか？

- A. 無効な生年月日で新規アカウント申請を提出しようとする
- B. 過去1ヶ月間に提出された新規口座開設申請について、生年月日が無効でないか確認してください。
- C. 生年月日フィールドの要件について、業務要件文書を確認してください。
- D. 生年月日フィールドの要件に関する構成設定を評価します。

Answer: ([解答を表示する](#)**)**

最新問題: 115

内部監査の質と正確性に関する継続的な懸念に対処するための最善の方法は、次のうちどれですか？

- A. 監査機能の独立したレビューを実施する。
- B. 監査作業書類のピアレビューを要求する。
- C. IS監査担当者のパフォーマンス管理を実施する。
- D. IS監査管理部門が終了会議を主導することを要求する。

Answer: ([解答を表示する](#)**)**

セクション：情報システムの監査プロセス

最新問題: 116

処理制御は、データの正確性と完全性を確保し、以下のどれを通してのみ処理されるかを保証します。最適な答えを選択してください。

- A. 文書化されたルーチン
- B. 承認済みルーチン
- C. 承認されたルーチン
- D. 承認されたルーチン

Answer: ([解答を表示する](#)**)**

説明／参考資料：

処理制御により、データの正確性と完全性が確保され、承認されたルーチンのみを通じて処理されることが保証されます。

最新問題: 117

サインオン手順には、固有のユーザーIDとパスワードの作成が含まれます。しかし、IS監査担当者は、多くの場合、ユーザー名とパスワードが同じであることを発見します。このリスクを軽減するための最善の対策は次のとおりです。

- A. 会社のセキュリティポリシーを変更する。

- B. 弱いパスワードのリスクについてユーザーに教育する。
- C. ユーザー作成時とパスワード変更時にこれを防ぐための検証機能を組み込みます。
- D. 一致しているユーザーIDとパスワードを定期的を確認し、検出と修正を行う必要があります。

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

最新問題: 118

監査作業の完了後、IS監査担当者は以下のことを行うべきである。

- A. 監査チームのメンバーに、調査結果の概要を配布する。
- B. 被監査者と作業書類を確認する。
- C. 被監査者に対し、初期調査結果を記載した報告書を提供する。
- D. 被監査者との協議に先立ち、上級管理職に報告書を提出する。

Answer: A ([メッセージを残す](#))

最新問題: 119

An organizations audit charter PRIMARILY:

- A. describes the auditors' authority to conduct audits.
- B. defines the auditors' code of conduct.
- C. formally records the annual and quarterly audit plans.
- D. documents the audit process and reporting standards.

Answer: A ([メッセージを残す](#))

An organization's audit charter primarily describes the auditors' authority to conduct audits. The audit charter is a formal document that defines the purpose, scope, responsibilities, and reporting relationships of the internal audit function. It also establishes the auditors' right of access to information, records, personnel, and physical properties relevant to their work. The audit charter provides the basis for the auditors' independence and accountability to the governing body and senior management.

最新問題: 120

最近の監査で、ある組織の情報セキュリティシステムが脆弱であり、監視を行っても侵入を検知できない可能性が高いと結論付けられました。以下のうち、最も適切な推奨事項はどれでしょうか？

- A. 機密データを暗号化し、システムを強化する
- B. 不要になった機密データを特定し、定期的に削除する
- C. 新たな犯罪行為や機密データへの攻撃を継続的に監視する。
- D. セキュリティおよび機密データの取り扱いに関する明確な方針を策定する

Answer: ([解答を表示する](#))

最新問題: 121

組織がデータ分類基準を策定する際に最も重要なことは、以下の点を確実にすることです。

- A. 組織のIT能力成熟度フレームワークに準拠する。
- B. 情報の認証に関する業務要件に基づいています。
- C. 組織の職務分掌要件に準拠する。
- D. 情報の機密性に関する業務上の要件に基づいています。

Answer: D ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 122

Which of the following should an IS auditor consider FIRST when evaluating firewall rules?

- A. The firewalls' default settings
- B. The organization's security policy
- C. The number of remote nodes
- D. The physical location of the firewalls

Answer: B ([メッセージを残す](#))

最新問題: 123

Ideally, stress testing should be carried out in a:

- A. test environment using test data.
- B. production environment using live workloads.
- C. test environment using live workloads.
- D. production environment using test data.

Answer: C ([メッセージを残す](#))

Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices Band D), and if only test data is used, there is no certainty that the system was stress tested adequately.

最新問題: 124

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- A. Report the risks to the CIO and CEO immediately
- B. Examine e-business application in development

- C. Identify threats and likelihood of occurrence
- D. Check the budget available for risk management

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence.

Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

最新問題: 125

Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

- A. DNS
- B. FTP
- C. SSH
- D. SMTP

Answer: A ([メッセージを残す](#))

Explanation/Reference:

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point -Internet service providers access internet using net access point. A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network.

You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer.

It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.

On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:

SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.

On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 273 and 274

従業員がポータブルメディア（MP3プレーヤー、フラッシュドライブなど）を使用する場合、情報システム監査担当者が最も懸念すべき点は何でしょうか？

- A. それらに機密データをコピーすること
- B. 楽曲や動画のコピー
- C. これらの機器の費用を全従業員で掛け合わせると高額になる可能性がある
- D. 企業ネットワークを通じて悪意のあるコードの拡散を促進する

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

MP3プレーヤーやフラッシュドライブに関する最大の懸念は、データ漏洩、特に機密情報の漏洩です。

これは、デバイスが紛失または盗難された場合に発生する可能性があります。楽曲や動画をコピーする際のリスクは著作権侵害ですが、これは通常、情報漏洩よりも重要度の低いリスクです。選択肢Cは、従業員が通常、ポータブルメディアを自費で購入するため、ほとんど問題になりません。選択肢Dは起こりうるリスクですが、情報漏洩ほど重要ではなく、他の対策で軽減できます。

最新問題: 127

IS管理部門は、既存の顧客関係システムを第4世代言語（4GL）を使用して書き換えることを決定しました。4GLを使用したシステム開発において、最も頻繁に発生するリスクは次のうちどれですか？

- A. 画面／レポートデザイン機能が不十分
- B. 複雑なプログラミング言語のサブセット
- C. オペレーティングシステム間での移植性の欠如
- D. データ集約型操作を実行できない

Answer: D ([メッセージを残す](#))

4GLは通常、データ集約型の処理には適していません。代わりに、主に次のような用途で使用されます。

グラフィカルユーザーインターフェース（GUI）の設計、またはシンプルなクエリ／レポート生成ツールとして使用できます。

不正解：

- A、B、スクリーン/レポート設計機能は4GLの主な利点の1つであり、4GLには単純なプログラミング言語のサブセット。
- C、携帯性も4GLの主な利点の1つです。

最新問題: 128

変更管理プロセスを評価するIS監査担当者は、変更ログからサンプルを選択する必要があります。監査担当者が変更ログが完全であることを確認するための最善の方法は何ですか？

- A. 変更管理担当者にインタビューして、完全性について確認する。
- B. ログから項目を1つ選び、システムまで遡って追跡します。
- C. 完全性に関する管理側の証明を取得する。
- D. システムから最後の変更を取得し、ログまで遡って追跡します。

Answer: (解答を表示する)

説明

正解はDです。監査担当者が変更ログが完全であることを確認する最善の方法は、システムから最後の変更を取得し、それをログまで遡って追跡することだからです。変更ログとは、ソフトウェアの更新、バグ修正、構成変更など、システムに対して行われたす

べての変更の記録です。変更ログには、変更の日時、変更の説明と目的、変更を行った担当者またはサービス、変更の承認状況などの情報が含まれている必要があります。完全な変更ログは、システムが安全で信頼性が高く、関連する規格や規制に準拠していることを保証するのに役立ちます。

変更管理プロセスを評価するIS監査担当者は、変更が適切に承認、文書化、テスト、実装されていることを確認するために、変更ログからサンプルを選択する必要があります。ただし、サンプルを選択する前に、監査担当者は変更ログが完全かつ正確であることを確認する必要があります。つまり、システムに加えられたすべての変更がログに記録されており、欠落、重複、または改ざんされたエントリがないことを確認する必要があります。これを行うために、監査担当者はバックワードトレーシングと呼ばれる手法を使用できます。これは、システムから最後の変更を取得し、それをログまで遡って追跡する手法です。この方法で、監査担当者は、変更が関連するすべての詳細とともにログに記録されているかどうか、またログに欠落や矛盾がないかどうかを確認できます。システムからの最後の変更がログに見つからない場合、またはログエントリと一致しない場合は、変更ログが不完全または不正確であることを示しています。

他の選択肢は、選択肢Dほど優れていません。変更管理担当者に完全性についてインタビューする（選択肢）方法は、主観的な意見や自己申告情報に依存するため、変更ログが完全であることを確認する信頼できる方法ではありません。これらの情報は真実または正確ではない可能性があります。ログから項目を取り出し、システムに遡って追跡する（選択肢）方法は、フォワードトレーシングと呼ばれる手法で、ログ内の特定の変更がシステムに実装されていることを検証するために使用できます。ただし、この手法では、システム内のすべての変更がログに記録されていることを確認できません。経営陣による完全性の証明を得る（選択肢C）方法は、完全性の証拠や検証を提供しないため、変更ログが完全であることを確認する十分な方法ではありません。経営陣による証明は、偏っていたり、利益相反の影響を受けたりする可能性もあります。

参考文献：

IS監査の基礎 :データプライバシーの監査

監査ログとは何か、そしてどのように機能するのか | Datadog

SOCにおける変更管理 :リスク、コントロール、監査、ガイダンス

監査機能を有効または無効にする | Microsoft Learn

#118 | ITGC - システム変更（監査ログレビュー - A2Q2

最新問題: 129

職務分掌の不備を検出する上で、以下の文書のうちどれが最も有用でしょうか？

- A. プロセスフローチャート
- B. システムフローチャート
- C. データフロー図
- D. エンティティ関係図

Answer: ([解答を表示する](#))

最新問題: 130

In a review of the organization standards and guidelines for IT management, which of the following should be included in an IS development methodology?

- A. Value-added activity analysis
- B. Risk management techniques
- C. Access control rules
- D. Incident management techniques

Answer: B ([メッセージを残す](#))

Risk management techniques should be included in an IS development methodology. An IS development methodology is a set of guidelines, standards, and procedures that provide a structured and consistent approach to developing information systems. A good IS development methodology should cover all the phases of the system development life cycle (SDLC), from planning and analysis to design, implementation, testing, and maintenance¹.

Risk management techniques are an essential part of an IS development methodology, as they help to identify, assess, prioritize, mitigate, monitor, and communicate the risks that may affect the success of the system development project. Risk management techniques can also help to ensure that the system meets the requirements and expectations of the stakeholders, complies with the relevant laws and regulations, and delivers value to the organization².

The other options are not as relevant or appropriate as risk management techniques for an IS development methodology. Value-added activity analysis is a technique for evaluating the efficiency and effectiveness of business processes, but it is not specific to IS development³. Access control rules are policies and mechanisms for restricting or granting access to information systems and resources, but they are more related to security management than IS development⁴. Incident management techniques are methods for handling and resolving incidents that disrupt the normal operation of information systems and services, but they are more related to service management than IS development⁵.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 1911

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 1942

* Value-Added Activity Analysis³

* Access Control Rules⁴

* Incident Management Techniques⁵

最新問題: 131

事業継続計画 (BCP) を策定する際、最初に実施すべきことは次のうちどれですか？

- A. 災害復旧計画 (DRP) を策定する
- B. 事業継続に関する研修を実施する。
- C. 操作を分類します。
- D. 事業影響分析 (BIA) を実施する

Answer: ([解答を表示する](#)**)**

最新問題: 132

The BEST way to prevent fraudulent payments is to implement segregation of duties between payment processing and:

- A. requisition creation.
- B. vendor setup.
- C. payment approval.
- D. check creation.

Answer: C ([メッセージを残す](#))

最新問題: 133

An IT service desk has recorded several incidents related to server downtime following the failure of a network time protocol (NTP) server. Which of the following is the BEST methodology to help identify the root cause?

- A. Crow-functional diagram
- B. Cause-and-effect diagram
- C. Server architecture diagram
- D. Data flow diagram

Answer: [\(解答を表示する\)](#)

最新問題: 134

内部監査管理部門が情報システム監査の品質を維持するために最も効果的な方法は、次のうちどれですか？

- A. IT管理部門と連携して、コントロール自己評価 (CSA)を実施する。
- B. 内部監査のためのバランススコアカードを導入する。
- C. 監査スタッフの年間業績評価に品質指標を含める。
- D. 第三者機関に依頼して、定期的な品質保証 (QA) レビューを実施してもらう。

Answer: D ([メッセージを残す](#))

最新問題: 135

組織の運用環境に新しいアプリケーションをリリースする前に、適切なテストが実施され、ロールバック計画が策定されていることを確認するために、次のうちどれを実施しておくべきでしょうか？

- A. 変更承認委員会
- B. 標準化された変更要求
- C. 独立した第三者機関による承認
- D. 安全なコードレビュー

Answer: A ([メッセージを残す](#))

包括的かつ詳細な手順説明：

変更承認委員会 (CAB)は、展開前に必要なすべてのテストとロールバック計画がレビューされていることを保証します。

* オプション A (正解): ACA は、アプリケーションが展開される前に変更がレビュー、テスト、承認され、リスクが最小限に抑えられることを保証します。これには、ロールバック計画が策定されていることを確認すること含まれます。

* Option B (Incorrect):Standardized change requestsare important but donot guarantee review and approvalby management and stakeholders.

* Option C (Incorrect):Third-party approvalmay be useful, but internalgovernance and control via a CABis more comprehensive.

* Option D (Incorrect):Secure code reviewshelp identify vulnerabilities, but they donot confirm proper deployment and rollback procedures.

Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation-Coverschange management and deployment best practices.

最新問題: 136

以下の活動のうち、IS監査人が独立性を維持しながら、統制自己評価 (CSA)を促進することを可能にするものはどれですか？

- A. 改善計画の実施
- B. 修復計画の策定
- C. CSAを部分的に完了する
- D. CSA質問票の開発

Answer: D ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 137

Which of the following provides the BEST assurance that security policies are applied across business operations?

- A. Organizational standards are required to be formally accepted.
- B. Organizational standards are enforced by technical controls.
- C. Organizational standards are included in awareness training.
- D. Organizational standards are documented in operational procedures.

Answer: D ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: 138

Which of the following actions should an organization's security policy require an employee to take upon finding a security breach?

- A. Report the incident to the manager immediately.
- B. Inform IS audit management immediately.
- C. Confirm the breach can be exploited.
- D. Devise appropriate countermeasures.

Answer: (解答を表示する)

Section: Protection of Information Assets

最新問題: 139

継続的デプロイメントプログラムの一環としてのセキュアなコードレビューは、どのタイプの制御に該当しますか？

- A. 論理
- B. 予防
- C. 修正
- D. 探偵

Answer: D ([メッセージを残す](#))

最新問題: 140

システム開発プロジェクトをレビューする監査担当者にとって、主要な高レベル目標は何ですか？

- A. プログラミング環境と処理環境が分離されていることを保証する
- B. プロジェクトに対する適切な承認が得られていることを確認する

- C. 事業目標の達成を確実にするため
- D. プロジェクトが効果的に監視・管理されるようにする

Answer: ([解答を表示する](#))

セクション：情報資産の保護

Explanation:

システム開発プロジェクトをレビューする監査担当者にとって、最も重要な高レベルの目標は、事業目標が達成されていることを確認することです。この目標は、他のすべてのシステム開発目標の指針となります。

最新問題: 141

IS監査担当者が、IS部門が正式に文書化された方法論、方針、および標準を使用していないことに気づいた場合、監査担当者は何をすべきでしょうか？最も適切な回答を選択してください。

- A. IT文書の不足は、通常、IT監査でテストされる統制にとって重要ではありません。
- B. 監査人は、少なくとも非公式な基準と方針を文書化すべきである。さらに、IS監査人は、実施すべき正式な文書化された方針を作成すべきである。
- C. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.
- D. The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

最新問題: 142

Which of the following findings should be of GREATEST concern to an IS auditor performing an information security audit of critical server log management activities?

- A. ログレコードは動的に異なるサーバーに分散されます。
- B. Logs are monitored using manual processes.
- C. ログ記録は、レビューされる前に上書きされる可能性があります。
- D. ログ記録手順の文書化が不十分である

Answer: ([解答を表示する](#))

最新問題: 143

インシデント対応計画の最初のステップは次のとおりです。

- A. 事件を検証する。
- B. IT部門の責任者に通知する。
- C. インシデントの影響を受けたシステムを隔離する。
- D. 根本原因分析を開始する。

Answer: A ([メッセージを残す](#))

説明

インシデント対応計画の最初のステップは通常、準備です¹²。しかし、提供されるオプションの中で、インシデントの検証が最初のステップとなるでしょう。これは、セキュリティイベントが実際にインシデントであることを確認することです³。誤検知でリソースを無駄にしないためにも、イベントを検証することが重要です。

参考文献：

インシデント対応計画 : フレームワークと手順 - CrowdStrike

インシデント対応とは？計画と手順 | マイクロソフト セキュリティ

インシデント対応計画の各段階とは？ - ISC2 ブログ

最新問題: 144

プライバシー監査において、IS監査担当者が行う最も重要なステップは次のうちどれですか？

- A. データ管理に関して実施されている管理体制を評価する。
- B. 従業員向けにプライバシー研修が実施されているかどうかを確認する。
- C. 適切な個人識別情報 (PII) 保護措置が講じられているか、第三者との契約内容を確認する。
- D. 個人識別情報 (PII) データのライフサイクルのすべての段階を分析し、潜在的なリスクを特定します。

Answer: D ([メッセージを残す](#))

プライバシー監査において最も重要なステップは、個人情報 (PII) の取り扱いに関連するすべてのリスクを特定することです。そのためには、収集、処理、保管、転送から保持、破棄に至るまで、個人情報データのライフサイクル全体を分析する必要があります。

選択肢A : データ管理統制のレビューは監査の一部ではあるが、ライフサイクル全体を対象とした監査よりも範囲が狭い。

選択肢B : プライバシーに関する研修は必要だが、研修だけではコンプライアンスを保証するものではない。

選択肢C : 第三者との契約内容を見直すことは重要ですが、アウトソーシングされたリスクのみを対象としています。

オプションD : あらゆる段階におけるプライバシーリスクを包括的にカバーします。

最新問題: 145

The MOST effective biometric control system is the one:

- A. which has the highest equal-error rate (EER).
- B. which has the lowest EER.
- C. for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- D. for which the FRR is equal to the failure-to-enroll rate (FER).

Answer: B ([メッセージを残す](#))

The equal-error rate (EER) of a biometric system denotes the percent at which the false-acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

最新問題: 146

侵入検知システム (IDS) の運用において最もよくある問題は以下のとおりです。

- A. 偽陽性の検出。
- B. トラップメッセージの受信。

- C. 拒否エラー率。
- D. サービス拒否攻撃。

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

IDS の構成と動作方法により、IDS の運用における主な問題は、実際にはセキュリティ インシデントではないイベントの認識 (検出)、つまり誤検知 (偽陽性) です。IS 監査担当者はこれを認識し、IDS チューニングなどの関連する制御の実装や、イベントがセキュリティ インシデントか誤検知かを判断するためのスクリーニング プロセスなどのインシデント処理手順を確認する必要があります。トラップ メッセージは、重要なイベントが発生したときに、Simple Network Management Protocol (SNMP) エージェントによって生成されますが、セキュリティや IDS とは特に関係ありません。拒否エラー 率は生体認証技術に関連しており、IDS とは関係ありません。サービス拒否は攻撃の一種であり、IDS の運用上の問題ではありません。

最新問題: 147

感染するファイルごとに自身を変化させる悪意のあるコードは、次のように呼ばれます。

- A. 論理爆弾。
- B. ステルスウイルス。
- C. トロイの木馬。
- D. 多型性ウイルス。

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

多型性ウイルスは、自身のコードを変化させる能力を持ち、多くの異なる亜種を持つことができる。一貫したバイナリパターンを持たないため、このようなウイルスを特定するのは困難である。

不正解：

- A. ロジックボムとは、プログラムやシステムに隠されたコードのことで、ユーザーが特定のアクションを実行したり、特定の条件が満たされたりしたときに何らかの動作を引き起こすものです。ロジックボムは、破損したシェアウェアやフリーウェアプログラムと一緒にダウンロードされることがあり、データの破壊、システムセキュリティの侵害、ハードドライブの消去などを引き起こす可能性があります。
- B. ステルスウイルスとは、ディスクアクセス要求を傍受することで自身を隠蔽するウイルスです。ウイルス対策プログラムがファイルやブートセクタを読み取ってウイルスを検出しようとする、ステルスウイルスはウイルス対策プログラムにファイルやブートセクタのクリーンなイメージを送りつけます。
- C. トロイの木馬とは、一見便利で無害に見えるウイルスプログラムですが、データの破壊や実行されているシステムのセキュリティ侵害など、有害な副作用があります。

最新問題: 148

災害の影響を予測するために、組織は以下のうちどれを行うべきでしょうか？

- A. リカバリポイント目標 (RPO) を定義する
- B. 災害復旧のシミュレーション
- C. 事業影響分析 (BIA) を作成する
- D. 能力成熟度モデルのギャップを分析する

Answer: C ([メッセージを残す](#))

事業影響分析 (BIA) とは、事業の中断や事故が組織に及ぼす可能性のある影響を特定し、評価するプロセスです。BIAは、組織がこうした潜在的な障害を理解し、準備するのに役立ち、問題が発生した際に迅速に対応し、正面から立ち向かうことを可能にします。BIAは、予期せぬ障害が発生した場合に何が起こるかを組織に示し、事業をできるだけ早く軌道に戻すための計画を立てることを可能にします。したがって、BIAは災害の影響を予測するための最良の選択肢と言えます。

参考文献：

* 10：事業影響分析(BIA) あらゆる事態に備える [2023] * Asana

* 11 :ビジネスインパクト分析 (BIA) の定義 - IT用語集 | ガートナー情報技術

* 12: ビジネス影響分析 (BIA) は、関連データを収集することにより、ビジネス、そのプロセス、およびシステムへの混乱の結果を予測する方法です。

最新問題: 149

包括的な情報システム監査ポリシーには、内部監査チームがどのような役割を担うべきかを詳細に定めたガイドラインを含めるべきである。

- A. 主要なOSアプリケーションの開発とコーディング。
- B. 主要なウェブアプリケーションの取得と保守。
- C. アプリケーション開発プロジェクトの人材管理サイクルにおいて。
- D. 主要アプリケーションの開発、取得、変換、およびテストにおいて。
- E. 選択肢のどれもでない。

Answer: D ([メッセージを残す](#))

監査方針には、主要アプリケーションの開発、取得、移行、テストにおいて内部監査がどのような役割を果たすかを詳細に定めたガイドラインを含めるべきである。このような方針は、有効性を確保するために経営陣の承認を得なければならない。

最新問題: 150

When developing customer-facing IT applications, in which stage of the system development life cycle (SLC) MOST beneficial to consider data privacy principles?

- A. Systems design and architecture
- B. User acceptance testing (UAT)
- C. Software selection and acquisition
- D. Requirements definition

Answer: ([解答を表示する](#))

最新問題: 151

組織の事業継続計画 (BCP) で対象とするシステムの優先順位を評価する際、IS監査担当者はまず以下の点を確認する必要があります。

- A. 過去の事業継続計画 (BCP) テストの結果をレビューする
- B. バックアップと復元プロセスを確認する
- C. 災害復旧サイト選定基準を確認する
- D. 復旧時間目標と復旧ポイント目標を検証する

Answer: D ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 152

Which of the following BEST enables alignment of IT with business objectives?

- A. Benchmarking against peer organizations
- B. Completing an IT risk assessment
- C. Leveraging an IT governance framework
- D. Developing key performance indicators (KPIs)

Answer: D ([メッセージを残す](#))

最新問題: 153

An IS auditor reviews an organizational chart PRIMARILY for:

- A. an understanding of workflows.
- B. investigating various communication channels.
- C. understanding the responsibilities and authority of individuals.
- D. investigating the network connected to different employees.

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation: An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

最新問題: 154

Which of the following BEST contributes to the quality of an audit of a business-critical application?

- A. Assigning the audit to independent external auditors
- B. Reviewing previous findings reported by the application owner
- C. Identifying common coding errors made by the development team
- D. Involving the application owner early in the audit planning process

Answer: D ([メッセージを残す](#))

Explanation

Involving the application owner early in the audit planning process is the best way to contribute to the quality of an audit of a business-critical application. The application owner has a deep understanding of the application and its business context, which

can provide valuable insights for the audit. Early involvement can also help ensure that the audit is aligned with the business objectives and risks, and that any potential issues are identified and addressed promptly¹².

References:

Business Critical Applications: An In-Depth Look

Framework for Audit Quality - IFAC

最新問題: 155

Which of the following is the most critical focus of a post-implementation review (PIR) for a newly modified IT application?

- A. Sufficiency of implemented controls
- B. Resource management plan
- C. Updates required for end-user manuals
- D. Rollback plans for changes

Answer: A ([メッセージを残す](#))

Comprehensive and Detailed In-Depth Explanation: A post-implementation review (PIR) of a newly modified IT application focuses on ensuring that the system meets business and security requirements effectively. The sufficiency of implemented controls (A) is the most critical aspect because it ensures that security, operational, and compliance controls are functioning correctly. These controls include access controls, data integrity checks, and audit logs to prevent unauthorized access, data corruption, or security breaches.

Other options:

- * Resource management plan (B) is important for project management but is not the primary concern for an IS auditor in a post-implementation review.
- * Updates required for end-user manuals (C) are necessary for usability but do not impact the security or operational integrity of the system.
- * Rollback plans for changes (D) are important for change management but are typically assessed before deployment, not in a PIR.

Reference: ISACA CISA Review Manual, IT Governance and Management of IT

最新問題: 156

IS監査人は、監査報告書を作成する際に、結果が以下の根拠に基づいていることを確認する必要があります。

- A. ISマネジメントからの声明。
- B. 他の監査人の作業書類。
- C. 組織統制の自己評価。
- D. 十分かつ適切な監査証拠。

Answer: D ([メッセージを残す](#))

ISACAの「報告」に関する基準では、IS監査人は報告結果を裏付ける十分かつ適切な監査証拠を保有する必要があると規定されています。IS管理部門からの声明は、実証的証拠で検証できない事項について合意を得るための根拠となります。監査人は他の監査人の作業文書にアクセスできる場合でも、報告書はレビューの過程で収集された証拠に基づいて作成されるべきです。組織統制自己評価 (CSA) の結果は、監査結果を補足することができます。選択肢A、B、Cは監査中に参照される可能性があります、それ自体では報告書を発行する十分な根拠とはみなされません。

最新問題: 157

ある企業がIT部門における職務分掌ポリシーを導入しました。役割ベースの環境において、アプリケーション開発者に割り当てられる可能性のある役割は次のうちどれでしょうか？

- A. ITオペレーター
- B. システム管理
- C. 緊急支援
- D. データベース管理

Answer: C ([メッセージを残す](#))

最新問題: 158

The objective of concurrency control in a database system is to:

- A. restrict updating of the database to authorized users.
- B. prevent integrity problems when two processes attempt to update the same data at the same time.
- C. prevent inadvertent or unauthorized disclosure of data in the database.
- D. ensure the accuracy, completeness and consistency of data.

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users, and controls such as passwords prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

最新問題: 159

IS監査担当者が前期の項目についてフォローアップ調査を行ったところ、経営陣が監査指摘事項に対処していなかったことが判明した。

IS監査担当者が次取るべき行動は次のうちどれでしょうか？

- A. 経営陣によって対応されなかった項目については、新しいレポートで例外として記録してください。
- B. 繰り返し見られる問題に対処するための代替案を提案する。
- C. 再発所見のリスク評価を実施する。
- D. 調査結果がなぜ対処されなかったのかを明らかにするため、経営陣にインタビューを行う。

Answer: ([解答を表示する](#)**)**

IS監査人が、経営陣が前期監査で指摘された事項に対処していないことを発見した場合、次の行動は、経営陣にインタビューを行い、なぜその指摘事項に対処しなかったのかを突き止めることである。これは、問題の根本原因、影響、およびリスクレベルを理解するのに役立つ。新しい報告書に例外事項を記載したり、代替案を提案したり、リスク評価を実施したりすることは、その後のステップとして考えられるが、経営陣へのインタビューの前に行うべきではない。参考文献 :CISAレビューマニュアル (デジタル版)、第1章、セクション1.6

最新問題: 160

大規模なITビジネスアプリケーションプロジェクトにおけるタスクの予算見積もりにおいて、以下のツールのうちどれが最も役立ちますか？

- A. ガントチャート
- B. ファンクションポイント分析 (FPA)
- C. クリティカルパス法 (CPM)
- D. バランススコアカード

Answer: B ([メッセージを残す](#))

最新問題: 161

仮想プライベートネットワーク (VPN)を使用することで、以下の制御目標のうちどれを最も効果的に満たすことができますか？

- A. 機密保持
- B. 完全性
- C. 入手可能性
- D. 否認禁止

Answer: ([解答を表示する](#)**)**

最新問題: 162

取引監査証跡の主な目的は以下のとおりです。

- A. 記憶媒体の使用量を削減する。
- B. 処理された取引に対する説明責任と責任を明確にする。
- C. IS監査人が取引を追跡するのを支援します。
- D. キャパシティプランニングに役立つ情報を提供する。

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

監査証跡を有効にすると、情報システムを通じて処理されたトランザクションを追跡することで、その説明責任と責任の所在を明確にすることができます。監査証跡を有効にすると、ディスク容量の使用が増加します。トランザクションログファイルはトランザクションの追跡に使用されますが、説明責任と責任の所在の特定には役立ちません。キャパシティプランニングの目的は、ITリソースを効率的かつ効果的に使用することであり、CPU使用率、帯域幅、ユーザー数などの情報が必要です。

最新問題: 163

リスクベースの監査戦略を策定する際に、情報システム監査担当者が最も重視すべき領域は次のうちどれですか？

- A. 重要なビジネスアプリケーション
- B. ビジネスプロセス
- C. 既存のIT統制
- D. 最近の監査結果

Answer: B ([メッセージを残す](#))

説明

これは、ビジネスプロセスが、組織が目標を達成し、ステークホルダーに価値を創造することを可能にする中核的な活動および機能であるためです。ビジネスプロセスはまた、組織のパフォーマンス、コンプライアンス、および評判に影響を与える可能性のあ

るさまざまなリスクの発生源および推進力でもあります。したがって、IS監査人は、組織の成功にとって最も重要、複雑、または脆弱なビジネスプロセスを理解、評価、および優先順位付けすることに焦点を当て、監査の目的、範囲、およびリソースをそれに応じて調整する必要があります¹²。

重要なビジネスアプリケーション A)は、IS監査人がリスクベースの監査戦略を策定する際に最も重要な焦点領域ではなく、むしろ注意が必要となる可能性のあるビジネスプロセスの特定の側面です。

重要なビジネスアプリケーションとは、企業資源計画 (ERP)、顧客関係管理 (CRM)、会計システムなど、ビジネスプロセスの実行と自動化をサポートするソフトウェアシステムのことです。重要なビジネスアプリケーションは、信頼性、セキュリティ、効率性に欠ける場合、組織に重大なリスクをもたらす可能性があります。そのため、IS監査人は、監査計画を策定する際に、ビジネスアプリケーションの重要性、機能性、および依存関係を考慮する必要がありますが、これらを主要な焦点とすべきではありません¹²。

既存のIT統制は、リスクベースの監査戦略を策定する際にIS監査人が最も重視する領域ではなく、リスク評価プロセスの成果または出力です。既存のIT統制とは、組織のビジネスプロセスや目標に影響を与える可能性のあるIT関連リスクを管理および軽減するために実施されるポリシー、手順、慣行、およびテクノロジーのことです。既存のIT統制は、その設計、有効性、成熟度において異なる場合があります。したがって、IS監査人は、監査の実施および報告プロセスの一部として既存のIT統制を評価およびテストする必要がありますが、それを主な焦点とすべきではありません¹²。

最近の監査結果 D)は、IS監査人がリスクベースの監査戦略を策定する際に最も重要な焦点領域ではなく、リスク評価プロセスのインプットまたは情報源です。最近の監査結果とは、組織のビジネスプロセス、リスク、およびコントロールに関する洞察やフィードバックを提供する可能性のある、過去の監査の所見、勧告、および意見のことです。最近の監査結果は、組織のリスクプロファイルまたは環境における変化や傾向を示す場合もあります。したがって、IS監査人は、監査計画およびスコープ設定プロセスの一部として最近の監査結果を確認し検討する必要がありますが、主な焦点として扱うべきではありません¹²。

最新問題: 164

Management has decided to accept a risk in response to a draft audit recommendation. Which of the following should be the IS auditor's NEXT course of action?

- A. Document management's acceptance in the audit report.
- B. Escalate acceptance to the audit committee.
- C. Escalate the acceptance to the board.
- D. Ensure a follow-up audit is on next year's plan.

Answer: ([解答を表示する](#))

最新問題: 165

コントロール自己評価 (CSA)の主な目的は以下のとおりです。

- A. 監査できない業務機能の保証を得る。
- B. 経営陣の分析を活用して監査リスクを排除する。
- C. 適切なアクセス制御が実施されていることを確認する。
- D. 各機能部門に対し、リスクと管理策について教育を行う。

Answer: D ([メッセージを残す](#))

最新問題: 166

Wi-Fi Protected Accessは、どのIEEE規格の大部分を実装していますか？

- A. 802.11i
- B. 802.11g
- C. 802.11x
- D. 802.11v

E. 選択肢のどれもでない。

Answer: ([解答を表示する](#))

セクション：情報資産の保護

説明

Explanation:

Wi-Fi Protected Access (WPA/WPA2)は、無線コンピュータネットワークを保護するためのシステムの一つです。IEEE 802.11i規格の大部分を実装しており、すべての無線ネットワークインターフェースカード（ただし、第一世代の無線アクセスポイントとは必ずしも互換性があるとは限りません）で動作するように設計されています。WPAがWEPよりも大きく改善された点の1つは、システムの使用状況に応じて鍵を動的に変更するTemporal Key Integrity Protocol (TKIP)です。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 167

IS監査人がフロントエンドの補助元帳とメイン元帳を調査しています。2つのシステム間で勘定科目のマッピングに欠陥がある場合、次のうちどれが最も大きな懸念事項となるでしょうか？

- A. 財務報告の不正確さ
- B. 単一のジャーナルエントリの二重投稿
- C. 新規取引をサポートできない
- D. アカунツ属性の不正な変更

Answer: ([解答を表示する](#))

最新問題: 168

IS監査担当者がサードパーティのITサービスプロバイダーに問題を発見した場合、最善の推奨事項は何でしょうか？
組織の人事 (HR) システムを外国でホストしている？

- A. プライバシー影響分析を実施する。
- B. 変更管理レビューを実施する。
- C. 第三者機関の監査報告書を確認する。
- D. 身元確認チェックを実施する。

Answer: A ([メッセージを残す](#))

セクション：情報システムの取得、開発、導入

最新問題: 169

Which of the following provides the MOST assurance of the integrity of a firewall log?

- A. The log is reviewed on a monthly basis.
- B. Authorized access is required to view the log.
- C. The log cannot be modified.
- D. The log is retained per policy.

Answer: C ([メッセージを残す](#))

The best way to provide assurance of the integrity of a firewall log is to ensure that the log cannot be modified.

A firewall log is a record of the traffic and events that occur at the firewall, which is a device or software that controls and filters the incoming and outgoing network traffic based on predefined rules and policies. The integrity of a firewall log means that the log is accurate, complete, consistent, and valid, and that it has not been altered, deleted, or corrupted by unauthorized or malicious parties. The IS auditor should verify that the firewall log has adequate controls to prevent or detect any modification of the log, such as encryption, hashing, digital signatures, write-once media, or tamper-evident seals. The other options are not as effective as ensuring that the log cannot be modified, because they either do not address the integrity of the log data, or they are monitoring or retention measures rather than preventive or detective controls. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

最新問題: 170

Which of the following BEST describes a digital signature?

- A. It is capable of authorization.
- B. It dynamically validates modifications of data.
- C. It is under control of the receiver.
- D. It is unique to the sender using it.

Answer: D ([メッセージを残す](#))

最新問題: 171

次のうち、ネットワークユーザーのパスワードを傍受するために使用できる手法はどれですか？

- A. 暗号化
- B. 匂いを嗅ぐ
- C. なりすまし
- D. データ消去

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

スニффイングとは、ネットワークを通過する機密情報（パスワードなど）を傍受するために用いられる攻撃手法です。暗号化とは、不正な第三者が通信内容を理解できないように情報を暗号化する手法です。スプーフィングとは、アドレスを偽造してパケットに挿入し、通信の発信元を偽装する手法です。データ消去とは、情報を消去したり、元の場所から削除したりする手法です。

最新問題: 172

Which of the following antispam filtering techniques would BEST prevent a valid, variable- length e-mail

message containing a heavily weighted spam keyword from being labeled as spam?

- A. Heuristic (rule-based)
- B. Signature-based
- C. Pattern matching
- D. Bayesian (statistical)

Answer: D ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Bayesian filtering applies statistical modeling to messages, by performing a frequency analysis on each word within the message and then evaluating the message as a whole. Therefore, it can ignore a suspicious keyword if the entire message is within normal bounds. Heuristic filtering is less effective, since new exception rules may need to be defined when a valid message is labeled as spam. Signature-based filtering is useless against variable-length messages, because the calculated MD5 hash changes all the time. Finally, pattern matching is actually a degraded rule-based technique, where the rules operate at the word level using wildcards, and not at higher levels.

最新問題: 173

システムの可用性という観点から見て、現代のクラウド環境における最大の利点は次のうちどれでしょうか？

- A. オンプレミスソリューションと比較して遅延が低減されます。
- B. オンデマンド容量管理が有効になっています。
- C. オンプレミスネットワークの容量が少なくて済みます。
- D. クラウドサーバーは内部サーバーよりも信頼性が高い。

Answer: B ([メッセージを残す](#))

最新のクラウド環境は、柔軟性の高いオンデマンドのキャパシティ管理機能を提供し、組織は需要に応じてリソースを自動的に増減させることができます。この柔軟性により、キャパシティ不足によるダウンタイムのリスクを最小限に抑え、ピーク時でもシステムの安定稼働を確保できます。

最新問題: 174

財務会計監査の過程で、情報システム監査人がIT全般統制に不備があることを発見した。

監査を完了するために最も効果的な方法はどれですか？

- A. 財務諸表の実質的検証を強化する。
- B. ITリスク評価を実施する。
- C. 統制の枠組みにより重点を置く。
- D. 財務アプリケーション管理への依存度を高める。

Answer: ([解答を表示する](#)**)**

最新問題: 175

An IS auditor has been asked to advise on the design and implementation of IT management best practices Which of the following actions would impair the auditor's independence?

- A. Designing an embedded audit module

- B. Providing consulting advice for managing applications
- C. Evaluating the risk management process
- D. Implementing risk response on management's behalf

Answer: D ([メッセージを残す](#))

最新問題: 176

内部監査チームと外部監査チームの両方が、リソースを最適化するために同じアプローチをレビューしている高リスク領域のIT全般統制監査中に、どのようなことが起こるでしょうか？

- A. 外部監査が実施した作業を内部監査テストに活用する。
- B. 内部監査人と外部監査人が同時に作業を行うようにしてください。
- C. 外部監査チームに内部監査の成果を活用するよう要請します。
- D. 統制監査を次年度の監査に繰り越す。

Answer: B ([メッセージを残す](#))

最新問題: 177

Which of the following is an example of a control that is both detective and preventive at the same time?

- A. Detection of unauthorized activity in a database prevents further manipulation by the database administrator (DBA).
- B. Detective fraud controls performed on past transactions prevent legal action being taken against the organization.
- C. A misconfiguration of an operating system is detected and future recurrence can successfully be prevented.
- D. A payment order to a sanctioned country is detected in the system before the payment is actually made.

Answer: ([解答を表示する](#))

最新問題: 178

Which of the following is the BEST control to ensure data entered into a calculation program is accurate?

- A. Programmed reasonableness checks with a data entry range
- B. Independent user review of test results
- C. Programmed edit checks to prevent entry of invalid data
- D. Visual verification of data entered

Answer: C ([メッセージを残す](#))

最新問題: 179

Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

- A. Data
- B. Segment
- C. Packet
- D. Frame

Answer: A ([メッセージを残す](#))

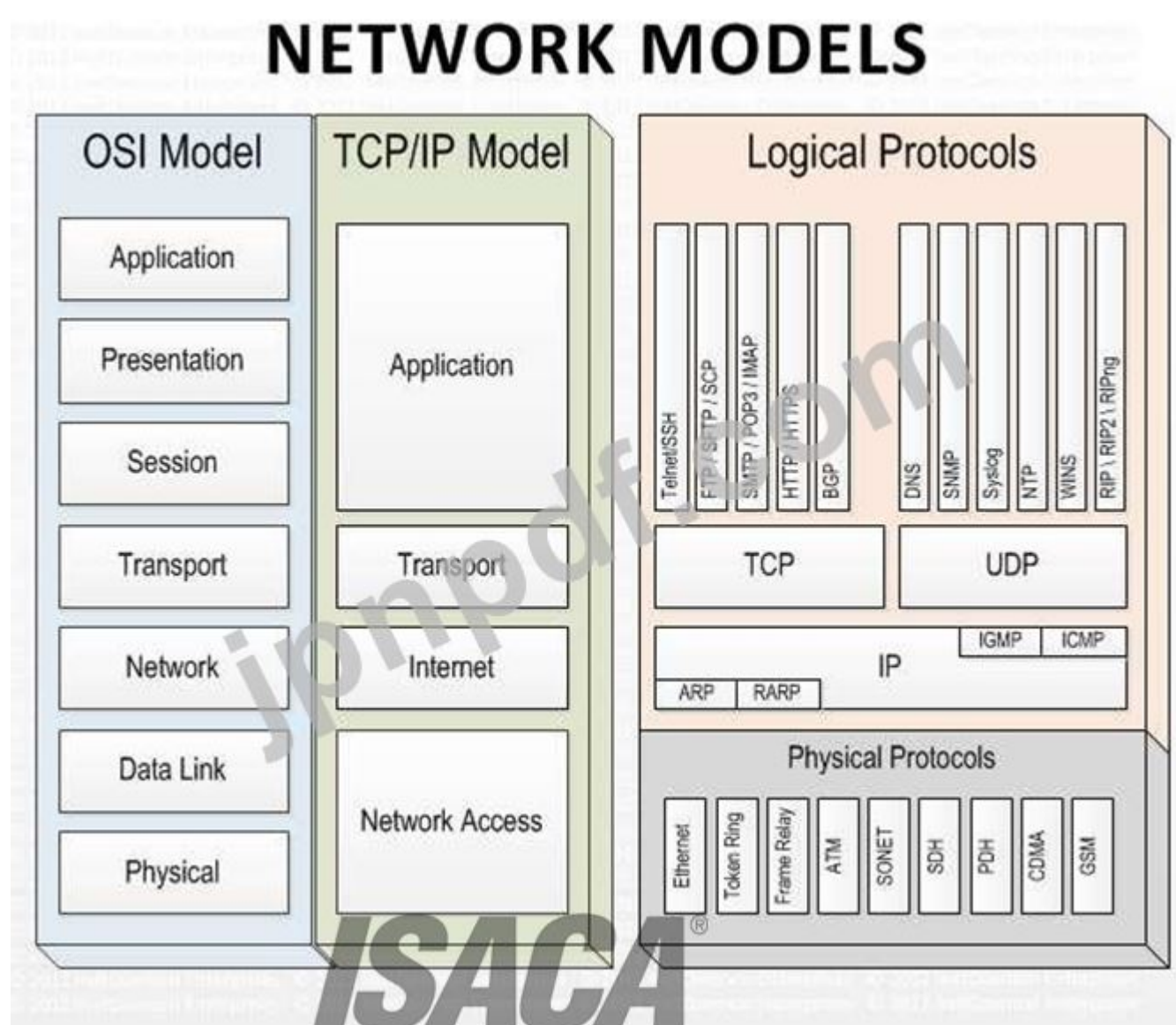
Section: Information System Operations, Maintenance and Support

Explanation:

Application layer's PDU is data.

For your exam you should know below information about TCP/IP model:

Network models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

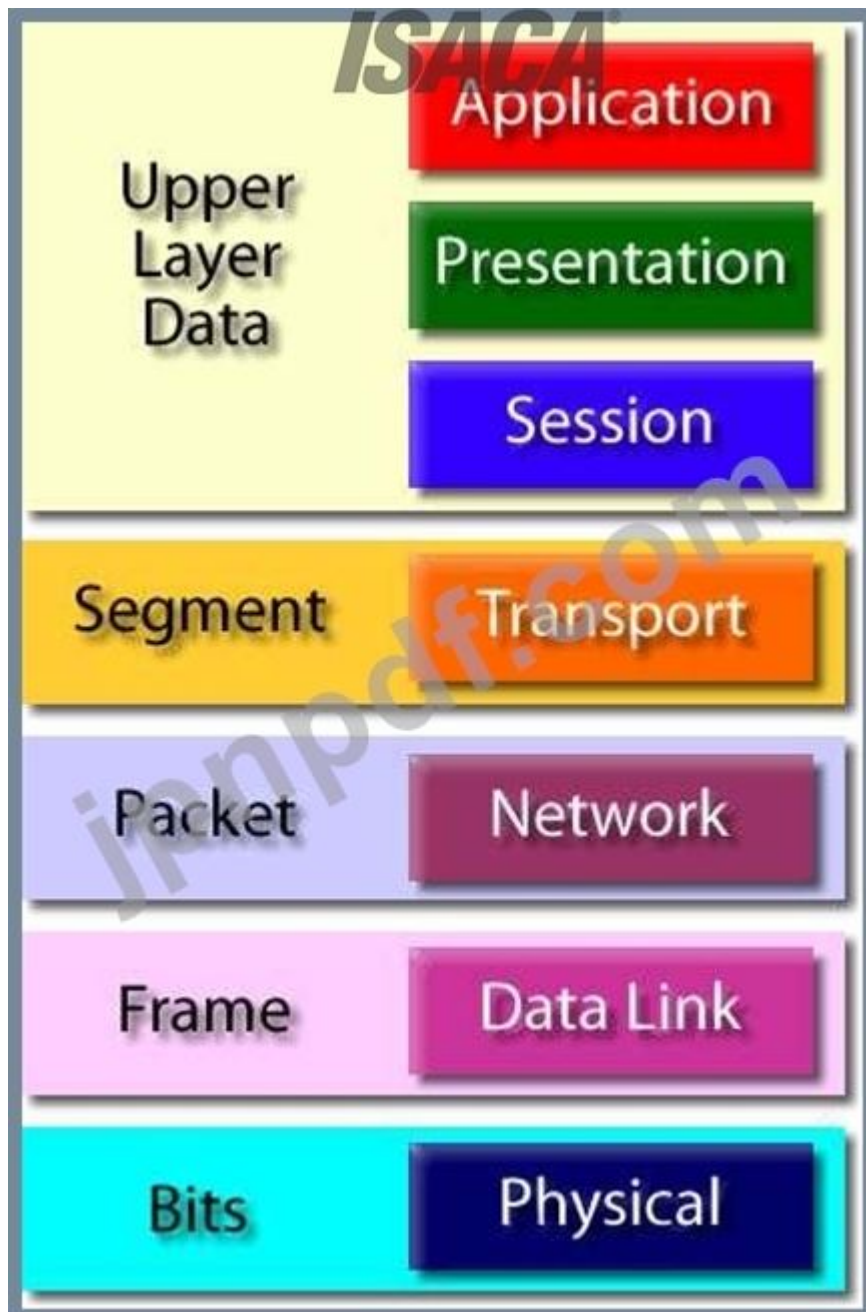
Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

Segment - Transport layer PDU

Packet - Network interface layer PDU

Frame/bit - LAN or WAN interface layer PDU

Reference:

CISA review manual 2014 page number 272

最新問題: 180

監査憲章には以下の内容が含まれるべきである。

- A. 技術や監査業務の変化する性質に合わせて、動的かつ頻繁に変化すること。
- B. 内部統制の維持およびレビューに関する監査目的と権限の委譲を明確に述べる。
- C. 計画された監査目標を達成するために設計された監査手順を文書化する。
- D. 監査機能の全体的な権限、範囲、責任を概説する。

Answer: D ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

監査憲章には、経営陣が情報システム監査に対して抱く目標と権限委譲を明記する必要があります。この憲章は、時間の経過とともに大きく変更されるべきではなく、経営陣の最高レベルで承認される必要があります。監査憲章は詳細なレベルのものではないため、具体的な監査目標や手順は含まれません。

最新問題: 181

Which of the following would BEST enable alignment of IT with business objectives?

- A. Monitoring key performance indicators (KPIs)
- B. Adopting industry best practices
- C. Completing an IT risk assessment
- D. Leveraging an IT framework

Answer: A ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 182

広範囲に複数のオフィスを持つ組織が、災害復旧計画 (DRP) を策定しました。実際の資源を用いて、DRPを最も費用対効果の高い方法でテストするには、次のうちどれが適切でしょうか？

- A. 完全動作テスト
- B. 準備テスト
- C. ペーパーテスト
- D. 回帰テスト

Answer: B ([メッセージを残す](#))

各地方事務所／地域では、災害復旧に向けた地方の業務体制の準備状況が適切かどうかを検証するために、準備状況テストが実施される。

最新問題: 183

A complex IS environment which of the following tasks should be performed by the data owner?

- A. Perform technical database maintenance.
- B. Perform data restoration when necessary.
- C. Test the validity of backup data
- D. Review data classifications periodically

Answer: ([解答を表示する](#))

最新問題: 184

What would be an IS auditor's BEST recommendation upon finding that a third-party IT service provider hosts the organization's human resources (HR) system in a foreign country?

- A. Conduct a privacy impact analysis.
- B. Implement change management review.
- C. Review third-party audit reports.
- D. Perform background verification checks.

Answer: A ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 185

Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

- A. ensure the employee maintains a good quality of life, which will lead to greater productivity.
- B. reduce the opportunity for an employee to commit an improper or illegal act.
- C. provide proper cross-training for another employee.
- D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

Answer: ([解答を表示する](#))

Section: Protection of Information Assets

Explanation:

Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

最新問題: 186

A source code repository should be designed to:

- A. prevent changes from being incorporated into existing code.
- B. prevent developers from accessing secure source code.
- C. provide secure versioning and backup capabilities for existing code.
- D. provide automatic incorporation and distribution of modified code.

Answer: C ([メッセージを残す](#))

A source code repository is a system that stores and manages the source code of a software project. A source code repository should be designed to provide secure versioning and backup capabilities for existing code, as these are essential features for concurrent development, code quality, and disaster recovery. Versioning allows developers to track, compare, and revert changes to the code over time. Backup ensures that the code is safely stored and can be restored in case of data loss or corruption.

References

Source Code Repositories: What is a Source Code Repository?

Git Source Code Repository Design Considerations

Best practices for repositories - GitHub Docs

最新問題: 187

IS監査担当者が、法律で定められた保存期間を超えて保持されている顧客記録が多数あることを発見した場合、個人データの過剰保存に伴うリスクに対処するための最善の方法は何でしょうか？

- A. 保存期間を過ぎた記録の自動削除を推奨します。
- B. 削除対象となる記録を特定するために、定期的な内部監査を実施する。
- C. 保管期間の不遵守を規制当局に報告する。
- D. 過剰保持の問題をデータプライバシー責任者にエスカレーションして対応を依頼する。

Answer: A ([メッセージを残す](#))

セクション :ITのガバナンスと管理

最新問題: 188

Which of the following is MOST important for an IS auditor to verify after finding repeated unauthorized access attempts were recorded on a security report?

- A. Password reset requests have been confirmed as legitimate
- B. There is evidence that the incident was investigated
- C. System configuration changes are properly tracked
- D. A comprehensive access policy has been established

Answer: B ([メッセージを残す](#))

Section: The process of Auditing Information System

最新問題: 189

An IS auditor reviewing database security should be MOST concerned if the database administrator (DBA):

- A. executes recovery procedures.
- B. assesses database performance.
- C. approves access roles.
- D. resolves database locks.

Answer: C ([メッセージを残す](#))

最新問題: 190

エンドユーザーコンピューティング (EUC)アプリケーションの開発において、よく見られるリスクは次のうちどれですか？

- A. アプリケーションはテストおよびIT全般管理の対象とならない場合があります
- B. 開発および維持費の増加
- C. アプリケーション開発時間の増加
- D. 情報要求への対応能力が低下するため、意思決定能力が損なわれる可能性がある。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

エンドユーザーが開発したアプリケーションは、システムアナリストによる独立した外部レビューを受けていない場合が多く、正式な開発手法に基づいて作成されていないことも少なくありません。そのため、適切な標準、管理体制、品質保証手順、および

ドキュメントが欠如している可能性があります。エンドユーザーアプリケーションのリスクの一つは、経営陣が従来型のアプリケーションと同様に、これらのアプリケーションに依存してしまう可能性があることです。エンドユーザーコンピューティング (EUC) システムは、一般的にアプリケーションの開発および保守コストの削減、そして開発サイクル時間の短縮につながります。また、EUCシステムは通常、経営陣からの情報要求に対する柔軟性と対応力を向上させます。

最新問題: 191

財務部門が使用している自動化された継続的監視プロセスの監査において、IS監査人が確認すべき最も重要な事項は次のうちどれですか？

- A. プロセスに組み込まれた二重管理と承認
- B. 監視ツールの設定
- C. テストドキュメントの管理承認
- D. 監視サービスの回復力

Answer: B ([メッセージを残す](#))

最新問題: 192

情報セキュリティプログラムの最も重要な成果は次のうちどれですか？

- A. 新たなセキュリティ技術はよりよく理解され、受け入れられるようになっている。
- B. 情報セキュリティリスクを軽減するためのコストが削減されます。
- C. 組織におけるセキュリティ責任に対する意識が向上する。
- D. オペレーティングシステムの脆弱性がより容易に特定される。

Answer: ([解答を表示する](#)**)**

最新問題: 193

データファイルの不正使用を防止する最も効果的な方法は何ですか？

- A. 自動ファイル入力
- B. テープライブラリアン
- C. アクセス制御ソフトウェア
- D. ロックされたライブラリ

Answer: ([解答を表示する](#)**)**

アクセス制御ソフトウェアは、データへの不正アクセスを防止するために設計された能動的な制御手段です。

最新問題: 194

複数階建てビルの上層階にある有人データセンターの防火対策を評価する際に、情報システム監査担当者が最も重視すべき事項は次のうちどれでしょうか？

- A. 目立つ場所に携帯型消火器が設置されていること
- B. 地元消防署による定期点検の記録
- C. テスト済みの緊急避難計画の文書化
- D. 施設全体の空調システムの適切性

Answer: ([解答を表示する](#)**)**

最新問題: 195

外部ITサービスプロバイダーの管理を監査するIS監査担当者にとって、以下のうちどれが最も重要な懸念事項となるべきでしょうか？

- A. 提供されるサービスのコストを最小限に抑える
- B. サービス提供者がサービスを再委託することを禁止する
- C. IT部門への知識移転プロセスの評価
- D. 契約どおりにサービスが提供されたかどうかを判断する

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

IS監査担当者の視点からすると、サービスプロバイダーの管理を監査する主な目的は、要求されたサービスが、許容可能で、円滑かつ契約上の合意に沿って提供されたかどうかを判断することです。コストの最小化は、適用可能で実現可能な場合（顧客のニーズに応じて）、従来IS監査担当者の業務範囲には含まれていません。これは通常、IT部門内のラインマネジメント機能が行います。さらに、監査の段階では、既存のプロバイダー契約のコストを最小化するには手遅れです。プロバイダーへの業務委託は懸念事項となる可能性があります、それが主な懸念事項ではありません。特定の状況下では、社内IT部門への知識移転が望ましい場合があります、ITサービスプロバイダーとその管理を監査する際のIS監査担当者の主な懸念事項となるべきではありません。

最新問題: 196

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

- A. Engaging an independent third party to perform the forensic investigation
- B. Restricting evidence access to professionally certified forensic investigators
- C. Documenting evidence handling by personnel throughout the forensic investigation
- D. Performing investigative procedures on the original hard drives rather than images of the hard drives

Answer: C ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 197

Which of the following would the IS auditor MOST likely review to determine whether modifications to the operating system parameters were authorized?

- A. Documentation of exit routines
- B. System initialization logs
- C. Change control log

D. Security system parameters

Answer: C ([メッセージを残す](#))

Operating system parameters are settings or values that affect the behavior or performance of the operating system¹.

Modifications to the operating system parameters may be necessary to improve the system functionality, security, or efficiency.

However, such modifications may also introduce risks or errors that can affect the system stability, compatibility, or integrity.

Therefore, modifications to the operating system parameters should be authorized and documented by the appropriate authority².

A change control log is a record of all changes made to the system, including the date, time, description, reason, authorization, and impact of each change³. A change control log can help the IS auditor to verify whether modifications to the operating system parameters were authorized by comparing the log entries with the actual system settings and the change approval documents⁴.

最新問題: 198

長年IS部門に勤務し、高度な技術的バックグラウンドと幅広い管理経験を持つ従業員が、IS監査部門の空席に応募しました。この人物を採用するかどうかは、その人物の経験と以下の点に基づいて判断する必要があります。

A. 勤続年数。これは技術的能力を確保するのに役立つため。

B. 年齢。監査技術のトレーニングは現実的ではない可能性がある。

C. IS知識。これは監査機能の信頼性を高めることになる。

D. IS監査人として、既存のIS関係から独立できる能力。

Answer: D ([メッセージを残す](#))

監査担当者と経営陣は、独立性を継続的に評価する必要があります。この評価では、個人的な関係の変化、経済的利害関係、過去の職務内容や責任といった要素を考慮に入れるべきです。従業員が情報システム部門で長年勤務してきたという事実だけでは、信頼性を保証するものではありません。監査部門のニーズを明確に定義し、候補者はその要件に基づいて評価されるべきです。勤務年数が長いからといって、技術的な能力が保証されるわけではありません。個人の年齢に基づいて資格を評価することは適切な基準ではなく、世界の多くの地域で違法です。

最新問題: 199

.IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

A. True

B. False

Answer: A ([メッセージを残す](#))

IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

最新問題: 200

Which of the following is MOST important to include in an awareness program focused on information security risk?

A. Social engineering attacks

B. Password parameters

C. Laptop theft prevention

D. Restricted websites

Answer: A ([メッセージを残す](#))

最新問題: 201

複数のマクロを含むスプレッドシートの正確性を評価する際に、情報システム監査担当者が最も重視すべき事項は次のうちどれですか？

A. スプレッドシートの暗号化

B. 主要計算の照合

C. マクロ内の数式

D. バージョン履歴

Answer: B ([メッセージを残す](#))

最新問題: 202

An IS auditor is preparing for a review of controls associated with a manufacturing plant's implementation of industrial Internet of Things (IoT) infrastructure. Which of the following vulnerabilities would present the GREATEST security risk to the organization?

A. Insufficient physical security around the IoT devices for theft prevention

B. Use of open-source software components within the IoT devices

C. Constraints in IoT device firmware storage space for code upgrades

D. IoT devices that are not using wireless network connectivity

Answer: B ([メッセージを残す](#))

The use of open-source software components in IoT devices presents the greatest security risk due to potential vulnerabilities that may exist within the software. These vulnerabilities can be exploited if patches are not applied promptly, and the organization might not have direct control over the software's maintenance and security updates. This risk is amplified in critical manufacturing environments where compromised IoT devices can lead to operational disruptions.

* Physical Security (Option A): While important, theft of IoT devices generally poses less risk compared to a system-wide compromise due to software vulnerabilities.

* Firmware Storage Constraints (Option C): While a limitation, this is a secondary concern compared to exploitable software.

* Devices Not Using Wireless Connectivity (Option D): Wired devices are generally more secure, reducing this as a significant concern.

Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題: 203

Which of the following backup schemes is the BEST option when storage media is limited?

A. Real-time backup

B. backup Differential

C. Virtual backup

D. Full backup

Answer: ([解答を表示する](#))

最新問題: 204

IS監査担当者にとって、以下の問題のうちどれが最も大きな懸念事項となるべきでしょうか？

IT災害復旧テストを見直していますか？

- A. 試験期間が限られていたため、最も重要なシステムのみが試験されました。その他のシステムは、残りの期間に別途試験されました。
- B. テスト中に、一部のバックアップシステムに欠陥があるか、動作していないことが判明し、これらのシステムのテストが失敗しました。
- C. バックアップサイトを起動する前に、元の生産サイトをシャットダウンして安全を確保する手順には、計画よりもはるかに多くの時間がかかりました。
- D. 毎年、同じ従業員がテストを実施します。参加者全員が各手順をよく理解しているため、復旧計画書は使用されません。

Answer: D ([メッセージを残す](#))

災害復旧テストでは、計画、プロセス、人員、IT システムをテストする必要があります。したがって、計画が使用されない場合、その正確性と妥当性を検証することはできません。災害復旧は、主要スタッフに依存してはなりません。災害は、彼らが利用できないときに発生する可能性があるためです。限られたテスト時間枠ですべてのシステムをテストできないことはよくあります。しかし、ビジネスに不可欠なシステムはテストされ、その他のシステムは最終的に年間を通じてテストされることが重要です。テストの目的の1つは、欠陥のあるデバイスを特定して交換し、災害時にすべてのシステムを交換できるようにすることです。選択肢Bは、発見された問題の数が体系的に非常に多い場合にのみ問題になります。実際の災害では、バックアップサイトを起動することが最優先事項であるため、元の本番環境を完全にシャットダウンする必要はありません。

最新問題: 205

アプリケーションベンダー契約において、ソースコードのエスクローを義務付ける条項が重要なのはなぜですか？

- A. システム開発環境と本番環境を分離する
- B. 著作権紛争から組織を守るため
- C. 必要なときに十分なコードが利用できるようにするため
- D. アプリケーションベンダーが倒産した場合でもソースコードが利用可能であることを保証するため

Answer: ([解答を表示する](#)**)**

セクション：情報資産の保護

Explanation:

アプリケーションベンダーとの契約において、ソースコードのエスクローを義務付ける条項を設けることは、アプリケーションベンダーが倒産した場合でもソースコードが確実に利用可能となるようにするために重要である。

最新問題: 206

IS監査担当者が継続的監視システムを導入する際に推奨される最初のステップは何ですか？

- A. 既存の内部統制を文書化する
- B. 内部統制のコンプライアンステストを実施する
- C. 管理監視運営委員会を設置する
- D. 組織内の高リスク領域を特定する

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

継続的監視システムを導入する際、IS監査担当者が最初に行うべきことは、組織内の高リスク領域を特定することである。

最新問題: 207

During a project audit, an IS auditor notes that project reporting does not accurately reflect current progress. Which of the following is the GREATEST resulting impact?

- A. The project steering committee cannot provide effective governance.
- B. The project reporting to the board of directors will be incomplete.
- C. The project manager will have to be replaced.
- D. The project will not withstand a quality assurance (QA) review.

Answer: A ([メッセージを残す](#))

最新問題: 208

組織のデータを分類するためのカテゴリは、次のうちどれに基づいて決定するのが最適でしょうか？

- A. 上級管理職によって処理された取引
- B. ビジネス機能に対する批判
- C. 個人識別データのセキュリティ要件の強化
- D. データの損失または漏洩によるビジネスへの影響

Answer: D ([メッセージを残す](#))

最新問題: 209

強力な認証の一般的な実装では、認証において以下の要素のうちどれを使用する可能性がありますか 3つ選択してください。

- A. あなたが知っていること」
- B. あなたが持っているもの」
- C. あなたらしさ」
- D. どの同じシステムで過去に実行したこと」
- E. どのシステムにインストールしたもの」
- F. 選択肢に該当しない。

Answer: A,B,C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

二要素認証 (2FA) とは、本人確認と権限付与のために2つの独立した方法を必要とする認証プロトコルを指します。二要素認証の一般的な実装では、2つの要素のうち1つとして「知っていること」を用い、もう1つとして「持っているもの」または「本人であること」を用います。実際、複数の要素を用いることは強力な認証とも呼ばれます。一方、1つの要素のみを用いることは、弱い認証とみなされる場合もあります。

最新問題: 210

Which of the following should be the FIRST step in managing the impact of recently discovered zero-day vulnerabilities?

- A. Identifying at-risk assets
- B. Assessing the impact of vulnerabilities
- C. Evaluating the likelihood of attack
- D. Estimating potential damage

Answer: A ([メッセージを残す](#))

The first step is to identify at-risk assets. Before an organization can assess impact, estimate damage, or evaluate likelihood, it must first determine which assets are exposed to the zero-day vulnerability. ISACA risk guidance emphasizes asset identification and security categorization as foundational steps in risk assessment.

In other words, you cannot meaningfully assess risk until you know what systems, applications, or services are affected.

Option A is correct because scoping the exposure comes first. Once at-risk assets are identified, the organization can prioritize remediation and then evaluate impact and likelihood in a focused way. ISACA's vulnerability and risk-related material supports risk-based prioritization built on asset visibility and understanding which systems are exposed.

Option B is not first because impact assessment depends on knowing which assets are vulnerable and how critical they are. Without that scope, impact analysis is incomplete.

Option C is also not first. Likelihood matters in risk analysis, but it comes after identifying the vulnerable environment and relevant exposure. ISACA's risk discussions place likelihood estimation after identifying assets, threats, and vulnerabilities.

Option D is similar to impact assessment and likewise depends on first knowing which assets are in scope.

Estimating damage without scoping exposure would be premature.

Therefore, A is the best answer because identifying the affected assets is the necessary first step in managing the impact of a newly discovered zero-day vulnerability.

References (Official ISACA):

* ISACA Journal, IT Asset Valuation, Risk Assessment and Control Implementation Model - asset identification and categorization precede likelihood and impact assessment.

* ISACA、「リスクベースのアプローチを使用して脆弱性修復の優先順位付けを行う」- 脆弱性への曝露が理解された後のリスクベースの優先順位付けをサポートします。

* ISACA、「運用技術分野の強化：実戦で実証されたサイバーレジリエンス戦略」- 悪用可能な弱点と露出した資産を特定することに重点を置いています。

* ISACAジャーナル、「サイバーセキュリティリスクの理解」- 脅威/脆弱性が特定された後、可能性と影響はリスクモデルの一部となります。

最新問題: 211

Which of the following should be done FIRST to effectively define the IT audit universe for an entity with multiple business lines?

- A. Identify key control objectives for each business line's core processes
- B. Obtain a complete listing of assets fundamental to the entity's businesses.
- C. Obtain a complete listing of the entity's IT processes
- D. Identify aggregate residual IT risk for each business line.

Answer: B ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 212

乾式消火システムを湿式システムよりも優先して使用する主な利点は、乾式システムには次のような利点があることです。

- A. 漏出のリスクが低減されています。
- B. 炎の抑制に効果的です。
- C. 抑制剤の放出を中止するための時間を延長します。
- D. 乾燥化学抑制剤のみを分散します。

Answer: (解答を表示する)

セクション: 情報資産の保護

最新問題: 213

Which of the following is MOST important for an IS auditor to review when determining whether IT investments are providing value to the business?

- A. Return on investment (ROI)
- B. Business strategy
- C. Business cases
- D. Total cost of ownership (TCO)

Answer: B (メッセージを残す)

Explanation

The answer B is correct because the most important thing for an IS auditor to review when determining whether IT investments are providing value to the business is the business strategy. The business strategy is the plan or direction that guides the organization's decisions and actions to achieve its goals and objectives.

The business strategy defines the organization's vision, mission, values, competitive advantage, target market, value proposition, and key performance indicators (KPIs).

IT investments are the expenditures or costs incurred by the organization to acquire, develop, maintain, or improve its IT assets, such as hardware, software, network, data, or services. IT investments can help the organization to support its business processes, operations, functions, and capabilities. IT investments can also help the organization to create or enhance its products, services, or solutions for its customers or stakeholders.

To determine whether IT investments are providing value to the business, an IS auditor needs to review how well the IT investments align with and contribute to the business strategy. Alignment means that the IT investments are consistent and compatible with the business strategy, and that they support and enable the achievement of the strategic goals and objectives. Contribution means that the IT investments are effective and efficient in delivering the expected outcomes and benefits for the business, and that they generate a positive return on investment (ROI) or value for money.

An IS auditor can use various methods or frameworks to review the alignment and contribution of IT investments to the business strategy, such as:

Balanced scorecard: A balanced scorecard is a tool that measures and monitors the performance of an organization across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help an IS auditor to

evaluate how well the IT investments support and improve each perspective of the organization's performance, and how they link to the organization's vision and strategy.

Value chain analysis: A value chain analysis is a tool that identifies and analyzes the primary and support activities that add value to an organization's products or services. A value chain analysis can help an IS auditor to assess how well the IT investments enhance or optimize each activity of the value chain, and how they create or sustain a competitive advantage for the organization.

Business case analysis: A business case analysis is a tool that evaluates the feasibility, viability, and desirability of a proposed project or initiative. A business case analysis can help an IS auditor to examine how well the IT investments address a business problem or opportunity, how they deliver the expected benefits and outcomes for the stakeholders, and how they compare with alternative options or solutions.

The other options are not as important as option B. **Return on investment (ROI)** (option A) is a metric that measures the profitability or efficiency of an investment by comparing its benefits or returns with its costs or expenses. ROI can help an IS auditor to quantify the value of IT investments for the business, but it does not capture all aspects of value, such as quality, satisfaction, or impact. ROI also depends on how well the IT investments align with the business strategy in the first place.

Business cases (option C) are documents that justify and support a proposed project or initiative by describing its objectives, scope, benefits, costs, risks, and alternatives. Business cases can help an IS auditor to understand the rationale and expectations for IT investments, but they do not guarantee that the IT investments will actually deliver the desired value for the business. Business cases also need to be aligned with the business strategy to ensure their relevance and validity. **Total cost of ownership (TCO)** (option D) is a metric that measures the total costs incurred by an organization to acquire, operate, maintain, and dispose of an IT asset over its life cycle. TCO can help an IS auditor to estimate the financial impact of IT investments for the business, but it does not reflect the benefits or outcomes of IT investments, nor does it indicate how well the IT investments support or enable the business strategy.

References:

IT Strategy: Aligning IT & Business Strategy

How To Measure The Value Of Your Technology Investments

IT Investment Management: A Framework for Assessing ... - GAO

How To Align Your Technology Investments With Your Business Strategy

最新問題: 214

Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

- A.** Resuming critical processes
- B.** Recovering sensitive processes
- C.** Restoring the site
- D.** Relocating operations to an alternative site

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

The resumption of critical processes has the highest priority as it enables business processes to begin immediately after the interruption and not later than the declared mean time between failure (MTBF).

Recovery of sensitive processes refers to recovering the vital and sensitive processes that can be performed manually at a tolerable cost for an extended period of time and those that are not marked as high priority. Repairing and restoring the site to

original status and resuming the business operations are time consuming operations and are not the highest priority. Relocating operations to an alternative site, either temporarily or permanently depending on the interruption, is a time consuming process; moreover, relocation may not be required.

最新問題: 215

ある組織がリモートワーク体制に移行しようとしています。その準備として、IT部門はリモートアクセスインフラストラクチャとシステムのストレステストとキャパシティテストを実施しています。どのような制御が実装されていますか？

- A. 指令
- B. 探偵
- C. 予防
- D. 補償

Answer: ([解答を表示する](#))

説明

ある組織がリモートワーク体制に移行しようとしています。その準備として、IT部門はリモートアクセスインフラストラクチャとシステムのストレステストとキャパシティテストを実施しています。このタイプの制御は、望ましい結果を達成するための行動を指示または誘導するために実装されています。したがって、これは指示的制御です。指示的制御は、望ましくない事象の発生を未然に防ぐための予防的制御です。これには、ポリシー、標準、手順、ガイドライン、トレーニング、テストが含まれます。検出的制御は、既に発生した望ましくない事象を特定するための事後的制御です。これには、監視、ログ記録、監査、レポート作成が含まれます。

予防的制御とは、望ましくない事象の発生を未然に防ぐための積極的な制御です。これには、認証、暗号化、ファイアウォール、ウイルス対策ソフトウェアなどが含まれます。補完的制御とは、主要な制御が実行不可能または費用対効果が低い場合に、主要な制御と同等のレベルの保護を提供する代替的な制御です。これには、職務分掌、手動レビュー、バックアップシステムなどが含まれます。参考文献 :CISAレビューマニュアル (デジタル版)、[ISACA用語集]

最新問題: 216

IS監査人が買掛金システムのリスクに対してコントロールをマッピングしています。
システムのエラーを検出する？

- A. 業務目標に沿ったプロセスの構築
- B. 新規支払いの品質管理レビュー
- C. 支払いの管理承認
- D. 入力検証

Answer: D ([メッセージを残す](#))

セクション：情報システムの監査プロセス

最新問題: 217

The majority of software vulnerabilities result from a few known kinds of coding defects, such as (Choose five.):

- A. buffer overflows
- B. format string vulnerabilities
- C. integer overflow

- D. code injection
- E. command injection
- F. None of the choices.

Answer: A,B,C,D,E ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

最新問題: 218

マイクロサービス指向アプリケーションの入力と出力を理解する上で、IS監査担当者にとって最も役立つのは次のうちどれですか？

- A. データフロー図
- B. ネットワークアーキテクチャ図
- C. ビジネス要件文書
- D. エンティティ関係図

Answer: A ([メッセージを残す](#))

包括的かつ詳細な説明：

マイクロサービスアーキテクチャにおいて、コンポーネント間のデータ移動を理解する最も効果的な方法は、データフロー図 (DFD) を用いることです。DFDは入力、出力、プロセス、データストアを明確に示し、監査担当者が分散サービス全体にわたるデータ移動を追跡するのに役立ちます。

- * オプションA：正解 DFDはアプリケーションの入力/出力を明確に示します。
- * オプションB :ネットワーク図はインフラストラクチャを示しますが、論理的なデータフローは示しません。
- * オプションC :ビジネス要件は、技術的な流れではなく、機能的なニーズを文書化する。
- * オプションD :ER図はデータベース構造を記述するものであり、プロセスフローを記述するものではありません。

ISACA 参考資料: CISA レビュー マニュアル第 27 版、ドメイン 3、監査分析におけるシステム ドキュメントとデータ フロー図に関するセクション。

最新問題: 219

What is often assured through table link verification and reference checks?

- A. Database integrity
- B. Database synchronization
- C. Database normalcy
- D. Database accuracy

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Database integrity is most often ensured through table link verification and reference checks.

最新問題: 220

重要な業務プロセスを実行するライセンスソフトウェアの契約を審査する情報システム監査担当者にとって、最大の懸念事項は何ですか？

- A. 契約には監査権条項は含まれていません。
- B. 運用レベル合意 (OLA)は交渉されなかった。
- C. 複数のベンダーの納品物が約束の期日を過ぎていました。
- D. ソフトウェアのエスクローは交渉されませんでした。

Answer: D ([メッセージを残す](#))

重要な業務プロセスを実行するライセンスソフトウェアの契約を審査するIS監査担当者にとって最大の懸念事項は、ソフトウェアエスクローが交渉されていないことです。ソフトウェアエスクローとは、第三者がライセンスソフトウェアのソースコードとドキュメントのコピーを安全な場所に保管する取り決めです。ソフトウェアエスクロー契約では、ライセンシーがエスクローされた資料にアクセスできる条件 (ライセンサーの破産、契約解除、契約違反など)が規定されています。ソフトウェアエスクローは、ライセンスソフトウェアに依存する重要な業務プロセスの継続性と可用性を確保するために重要です。ソフトウェアエスクローがない場合、ライセンシーは、ライセンサーとの間で何らかの障害や紛争が発生した場合に、ソフトウェアの保守、変更、復旧において重大なリスクと課題に直面する可能性があります。参考文献：

CISA試験対策マニュアル (デジタル版)

CISAに関する質問、回答、解説データベース

最新問題: 221

When reviewing the monitoring and prevention of sensitive data moving out of an organization's network, which of the following is MOST important for an IS auditor to verify?

- A. Transport Layer Security (TLS) is used
- B. Firewall rules have been documented
- C. Deep packet inspection is enabled
- D. Chain of custody is followed

Answer: C ([メッセージを残す](#))

Deep packet inspection provides the ability to examine packet payloads for sensitive content (not just headers), enabling detection and blocking of confidential data in motion. Without DPI, encrypted or non-standard traffic could bypass perimeter controls, undermining any monitoring or prevention efforts.

最新問題: 222

組織内でITガバナンス戦略を導入することによる最大のメリットは次のうちどれですか？

- A. 従業員は役割と責任を理解している
- B. 経営陣はIT関連のリスクを認識している。
- C. ITプロジェクトは予定通りかつ予算内で完了する。
- D. 報告と指標の優先順位が高くなります。

Answer: C ([メッセージを残す](#))

最新問題: 223

情報システム監査の結果、新たに導入されたアプリケーションのデフォルトパスワードが変更されていないことが判明した。フォローアップ監査中に、
以下の内容は、調査結果が効果的に対処されたことを示す最良の証拠となるでしょうか？

- A. アプリケーションユーザーにパスワード変更を求めるシステム生成メール
- B. 次回ログイン時にパスワード変更が必要なシステムパラメータのスクリーンショット
- C. パスワード変更を記録したアプリケーションログファイル
- D. パスワードが変更されたことを管理者が書面で確認する

Answer: ([解答を表示する](#))

最新問題: 224

What a the BEST control to address SOL injection vulnerabilities?

- A. Unicode translation
- B. Secure Sockets Layer (SSL) encryption
- C. Input validation
- D. Digital signatures

Answer: ([解答を表示する](#))

最新問題: 225

認証局 (CA) は、以下のプロセスを委任することができます。

- A. revocation and suspension of a subscriber's certificate.
- B. generation and distribution of the CA public key.
- C. establishing a link between the requesting entity and its public key.
- D. issuing and distributing subscriber certificates.,

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Establishing a link between the requesting entity and its public key is a function of a registration authority.

This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform.

Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

最新問題: 226

以下のうち、実行された行為に対する責任を回避し、否認を不可能にするものは何でしょうか？

- A. 適切な認証
- B. 適切な識別と認証
- C. 適切な識別
- D. 適切な識別、認証、および認可

Answer: B ([メッセージを残す](#))

説明／参考資料：

アクセス制御において適切な本人確認と認証が行われない場合、行われたいかなる行為についても責任を問うことはできません。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **227**

To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

- A. examine the change control system records and trace them forward to object code files.
- B. review access control permissions operating within the production program libraries.
- C. examine object code to find instances of changes and trace them back to change control records.
- D. review change approved designations established within the change control system.

Answer: C ([メッセージを残す](#))

The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes. The other choices are valid procedures to apply in a change control audit but they do not directly address the risk of unauthorized code changes.

最新問題: **228**

ほとんどのITサービスが外部委託されている環境において、事業継続計画を最も適切に管理する方法は次のとおりです。

- A. IT管理、
- B. 事業継続計画の専門家。
- C. 経営管理
- D. アウトソーシングサービスプロバイダーの管理

Answer: ([解答を表示する](#))

最新問題: **229**

組織の活動が計画レベルや期待レベルと異なるかどうかを、情報システム管理部門が判断するためのプロセスとはどのようなものか？

- A. 事業影響評価
- B. リスク評価
- C. IS評価方法
- D. 主要業績評価指標 (KPI)

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

IS評価手法を用いることで、IS管理者は組織の活動が計画レベルや期待レベルと異なっているかどうかを判断できる。

最新問題: 230

ITインフラストラクチャのパフォーマンス、リスク、および能力は、以下の方法で測定するのが最適です。

- A. リスク管理レビュー
- B. サービスレベル契約 (SLA)。
- C. 自己評価コントロール (CSA)。
- D. バランススコアカード。

Answer: C ([メッセージを残す](#))

最新問題: 231

Which of the following would provide multi-factor authentication for physical access to a data center?

- A. Key card with owner's photo on it
- B. Facial recognition and presence of a security guard
- C. Retina scan and voice recognition
- D. Proximity badge and fingerprint scan

Answer: D ([メッセージを残す](#))

最新問題: 232

A new regulatory standard for data privacy requires an organization to protect personally identifiable information (PII). Which of the following is MOST important to include in the audit engagement plan to access compliance with the new standard?

- A. Identification of IT systems that host PII
- B. Review of data loss risk scenarios
- C. Identification of unencrypted PII
- D. Review of data protection procedures

Answer: D ([メッセージを残す](#))

Section: Governance and Management of IT

最新問題: 233

"Under the concept of ""defense in depth"", subsystems should be designed to:"

- A. ""fail insecure""
- B. ""fail secure""
- C. ""react to attack""
- D. ""react to failure""
- E. None of the choices.

Answer: B ([メッセージを残す](#))

"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure""."

最新問題: 234

Which of the following human resources management practices BEST leads to the detection of fraudulent activity?

- A. Background checks
- B. Time reporting
- C. Employee code of ethics
- D. Mandatory time off

Answer: D ([メッセージを残す](#))

Section: Governance and Management of IT

最新問題: 235

An advantage of the use of hot sites as a backup alternative is that:

- A. the costs associated with hot sites are low.
- B. hot sites can be used for an extended amount of time.
- C. hot sites can be made ready for operation within a short period of time.
- D. they do not require that equipment and systems software be compatible with the primary site.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution, and requires that equipment and systems software be compatible with the primary installation being backed up.

最新問題: 236

次のうち、ソーシャルエンジニアリング攻撃の潜在的な影響を軽減するものはどれですか？

- A. 規制要件への準拠
- B. 倫理的理解の促進
- C. セキュリティ意識向上プログラム
- D. 効果的な業績インセンティブ

Answer: C ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

ソーシャルエンジニアリングはユーザーを欺くことを基本としているため、最善の対策または防御策はセキュリティ意識向上プログラムです。その他の選択肢はユーザー中心ではありません。

最新問題: 237

施設全体に設置された乾式配管システムを通して、主弁から放出された水によって火災を抑制する消火システムの種類は何ですか？

- A. 乾式スプリンクラーシステム
- B. 散水式スプリンクラーシステム

C. 湿式配管システム

D. ハロンスプリンクラーシステム

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

最新問題: 238

データベースセキュリティレビューの予備計画段階において、情報システム監査担当者は最初にどのタスクを完了すべきでしょうか？

A. 最も重要なデータベース制御を特定する

B. 使用されているデータベースの種類を評価する

C. 事業影響分析 (BIA)を実施する

D. 対象となるデータベースを決定する

Answer: D ([メッセージを残す](#))

最新問題: 239

以下のファイアウォールのうち、ハッカーの侵入に対する最も高いレベルの制御を提供するものはどれですか？

A. 回路ゲートウェイ

B. アプリケーションレベルゲートウェイ

C. パケットフィルタリングルーター

D. スクリーニングルーター

Answer: B ([メッセージを残す](#))

説明

ハッカーの侵入に対する制御を最も効果的に行うファイアウォールは、アプリケーションレベルゲートウェイです。ファイアウォールとは、事前に定義されたルールやポリシーに基づいてネットワークトラフィックをフィルタリングまたはブロックするデバイスまたはソフトウェアです。ファイアウォールは、情報システムやネットワークをハッカーやその他の悪意のあるエンティティによる不正アクセスや攻撃から保護するのに役立ちます。アプリケーションレベルゲートウェイは、ネットワークモデルのアプリケーション層（レイヤー7）で動作するファイアウォールの一種です。アプリケーション層は、ユーザーアプリケーションがネットワーク上で相互に通信する層です。アプリケーションレベルゲートウェイは、プロトコル、コマンド、リクエスト、レスポンスなど、アプリケーションレベルで各ネットワークパケットの内容とコンテキストを検査および分析し、特定の基準や条件に基づいてアクセスを許可または拒否することで、ハッカーの侵入に対する制御を最も効果的に行います。アプリケーションレベルゲートウェイは、認証、暗号化、キャッシング、ログ記録などの追加機能も実行でき、ネットワークトラフィックのセキュリティとパフォーマンスを向上させます。

サーキットゲートウェイは、ネットワークモデルのトランスポート層（レイヤー4）で動作するファイアウォールの一種です。この層では、ネットワークを介してエンドポイント間でデータが転送されます。サーキットゲートウェイは、2つのエンドポイント（クライアントとサーバーなど）間に安全な接続を確立し、パケットの内容を検査または分析することなくパケットを中継することで、ハッカーの侵入に対する中程度の制御を提供します。サーキットゲートウェイは、暗号化、認証、アドレス変換などの機能を実行して、ネットワークトラフィックのセキュリティとプライバシーを向上させることもできます。パケットフィルタリング

ルータは、ネットワークモデルのネットワーク層（レイヤー3）で動作するファイアウォールの一種です。この層では、異なるネットワークまたはサブネット間でデータがルーティングされます。パケットフィルタリングルータは、各ネットワークパケットのヘッダーを検査し、送信元アドレス、宛先アドレス、ポート番号、プロトコルなどの基本基準に基づいてアクセスを許可または拒否することで、ハッカーの侵入に対する低レベルの制御を提供します。パケットフィルタリングルータは、ルーティング、転送、アドレス変換などの機能を実行して、ネットワークトラフィックの配信と効率を最適化することもできます。スクリーニングルータは、ネットワークモデルのネットワーク層（レイヤー3）で動作するファイアウォールの一種です。レイヤー3は、異なるネットワーク間またはサブネット間でデータがルーティングされる層です。スクリーニングルータは、各ネットワークパケットのヘッダーを検査し、送信元アドレス、宛先アドレス、ポート番号、プロトコルなどの基本基準に基づいてアクセスを許可または拒否することで、ハッカーの侵入に対する制御を低レベルで提供します。また、スクリーニングルータは、ルーティング、転送、アドレス変換などの機能を実行して、ネットワークトラフィックの配信と効率を最適化することもできます。

最新問題: 240

IS監査担当者がアプリケーションシステムの導入後レビューを実施するよう割り当てられました。

以下の状況はIS監査人の独立性を損なう可能性があったか？ IS監査人：

- A. アプリケーションシステムの開発中に特定の制御を実装しました。
- B. アプリケーションシステムの監査専用の組み込み監査モジュールを設計しました。
- C. アプリケーションシステムプロジェクトチームのメンバーとして参加したが、運用には携わらなかった。責任。
- D. アプリケーションシステムのベストプラクティスに関するコンサルティングアドバイスを提供しました。

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

IS監査人が開発に積極的に関与している、または関与していた場合、独立性が損なわれる可能性があります。アプリケーションシステムの取得と実装。選択肢BとCは、IS監査人の独立性。選択肢Dは、IS監査人の独立性が損なわれることはないため誤りです。既知のベストプラクティスに関するアドバイスを提供することによって。

最新問題: 241

組織が新規従業員に対し、適用されるプライバシーおよびデータ保護規制に関する研修の受講を義務付ける場合、どのような種類の管理が行われていると言えるでしょうか？

- A. 探偵制御
- B. 予防的管理
- C. 補正制御
- D. 指示制御

Answer: D ([メッセージを残す](#))

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 242

次のうち、ソーシャルエンジニアリング攻撃の手法はどれですか？

- A. 許可されていない人物が、許可された人物の後についてセキュリティドアを通してセキュリティ施設への不正アクセスを試みる。
- B. 従業員が電話で質問に答えることで、機密のIPアドレスとパスワードを漏洩するように誘導される。
- C. ハッカーがスキャンツールを使ってオフィスビル内を歩き回り、無線ネットワークを探してアクセス権を得ようとしている。
- D. 侵入者がネットワークを流れる機密情報を盗聴・収集し、第三者に販売する。

Answer: B ([メッセージを残す](#))

説明

従業員は電話で質問に答えることで、機密のIPアドレスやパスワードを漏らすよう誘導されます。これは、従業員の信頼や好奇心を利用して、ネットワークへのアクセスや侵害に利用できる機密情報を入手するソーシャルエンジニアリング攻撃の手法です。ウェブ検索結果によると、ソーシャルエンジニアリングとは、心理操作を用いてユーザーを騙し、セキュリティ上のミスをさせたり、機密情報を漏らさせたりする技術です¹。フィッシング、ホエーリング、ベイト、プリテキスティングは、ソーシャルエンジニアリング攻撃の一般的な形態です²。ソーシャルエンジニアリング攻撃は、システムの脆弱性ではなく人的ミスに依存するため、純粋な技術的攻撃よりも効果的で収益性が高い場合が多いです。

最新問題: 243

Overall business risk for a particular threat can be expressed as:

- A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
- B. the magnitude of the impact should a threat source successfully exploit the vulnerability.
- C. the likelihood of a given threat source exploiting a given vulnerability.
- D. the collective judgment of the risk assessment team.

Answer: A ([メッセージを残す](#))

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

最新問題: 244

IS監査担当者は、既存システムを置き換える新しい医療記録システムに関連する最も重要なリスクとして、次のうちどれを考慮すべきでしょうか？

- A. データが正しく変換されず、患者記録が不正確になります。
- B. 導入プロジェクトは大幅な予算超過となり、予算予測を上回りました。
- C. スタッフが調達プロセスに関与していなかったため、新しいシステムに対するユーザーの抵抗が生じました。
- D. 新システムには容量の問題があり、ユーザーの応答時間が遅くなっています。

Answer: ([解答を表示する](#))

最新問題: 245

継続的インテグレーション／継続的開発（CI/CD）プロセスは、ソフトウェア障害のリスクを低減するのにどのように役立つのでしょうか？

- A. ソフトウェアバージョンのロールバックが容易
- B. より小さな段階的变化
- C. 手動によるマイルストーンの削減
- D. 自動ソフトウェアテスト

Answer: B ([メッセージを残す](#))

説明

継続的インテグレーション/継続的開発 (CI/CD) プロセスは、大規模で頻繁でないアップデートではなく、ソフトウェア コードへの小規模な増分変更を可能にすることで、ソフトウェア障害のリスクを低減するのに役立ちます 12。小規模な増分変更により、開発者はエラー、バグ、脆弱性をより迅速かつ容易に検出して修正し、ソフトウェアが常に動作状態にあることを保証できます 34。小規模な増分変更は、ソフトウェア開発プロセスの複雑さと不確実性を低減し、ソフトウェア製品の品質と信頼性を向上させます 5。

参考文献

1: CI/CDとは？継続的インテグレーションと継続的デリバリーの説明1 2: CI/CDの5つの課題とその解決策 | TechBeacon4 3: 継続的インテグレーション vs 継続的デリバリー vs 継続的デプロイメント2 4: CI/CDの7つの課題とその必須ソリューション | BrowserStack3 5: CI/CDの5つのよくある落とし穴とその回避方法 | InfoWorld5

最新問題: 246

以下の技術のうち、デバイス間のデータ伝送における最大通信距離が最も短いのはどれですか？

- A. Bluetooth
- B. Wi-Fi
- C. 近距離無線通信（NFC）
- D. 長期進化（LTE）

Answer: C ([メッセージを残す](#))

最新問題: 247

遠隔コールセンターとの顧客データベースの双方向レプリケーションに関する提案プロジェクトを評価する際、IS監査担当者は以下の点を確認する必要があります。

- A. データベースの競合はレプリケーション中に処理されます。
- B. エンドユーザーは複製プロセスについてトレーニングを受けます。
- C. ソースデータベースは両方のサイトにバックアップされています。
- D. 両方のデータベースでユーザー権限は同一です。

Answer: A ([メッセージを残す](#))

データベースの競合とは、顧客データベースとリモートコールセンターデータベースなど、2つの異なるサーバーで同じデータが変更され、その変更内容が一致しない場合に発生します。例えば、顧客が顧客データベースで電話番号を更新し、コールセンターのエージェントが同じ顧客の住所をリモートコールセンターデータベースで更新した場合、2つの更新内容に競合が生じます。データベースの競合は、適切に検出 解決されない場合、データの不整合、破損、または損失を引き起こす可能性があります。

双方向レプリケーションとは、2つのデータベース間でデータを同期するプロセスであり、一方のデータベースで行われた変更がもう一方のデータベースにも反映され、その逆も同様です。双方向レプリケーションは、データの可用性、パフォーマンス、および拡張性を向上させることができますが、データベースの競合のリスクも高めます。したがって、リモートコールセンターとの顧客データベースの双方向レプリケーションに関する提案プロジェクトを評価する際には、IS監査担当者は、レプリケーション中にデータベースの競合が適切に管理されていることを確認する必要があります。つまり、プロジェクトには、以下の事項について明確かつ効果的な戦略が必要です。

ロック、タイムスタンプ、パーティショニングなどの技術を用いて、データベースの競合を防止または最小限に抑える。

トリガー、ログ、アラートなどのツールを使用して、データベースの競合を検出または特定する。

優先度ベース、ルールベース、ユーザーベースなどの解決方法を用いて、データベースの競合を解決または処理する。

その他の選択肢は以下のとおりです。

B) エンドユーザーがレプリケーションプロセスについてトレーニングを受けていること :これは、リモートコールセンターとの顧客データベースの双方向レプリケーションに関する提案プロジェクトを評価する際に、IS監査人が確認すべき関連性のある重要な要素ではありません。エンドユーザーはレプリケーションプロセスに直接関与するわけではなく、レプリケーションの仕組みに関する詳細な知識やスキルも必要ありません。レプリケーションプロセスはエンドユーザーにとって透過的かつシームレスであるべきであり、エンドユーザーはアプリケーションまたはインターフェースを通じてのみデータとやり取りすればよいのです。

C) ソースデータベースが両サイトでバックアップされていること :これは、リモートコールセンターとの顧客データベースの双方向レプリケーションの提案プロジェクトを評価する際に、IS監査人が確認すべき十分条件でも必要条件でもありません。ソースデータベースを両サイトでバックアップすることで、ある程度のデータ保護と復旧は可能になりますが、レプリケーション中に発生する可能性のあるデータベースの競合の問題には対処できません。さらに、ソースデータベースを両サイトでバックアップすることは、ストレージ容量とネットワーク帯域幅を多く消費し、レプリケーションプロセスに複雑さとオーバーヘッドをもたらす可能性があるため、実現可能または効率的ではない場合があります。

D) 両方のデータベースでユーザー権限が同一であること :これは、リモートコールセンターとの顧客データベースの双方向レプリケーションの提案プロジェクトを評価する際に、IS監査人が確認すべき重要または関連性の高い要素ではありません。ユーザー権限とは、ユーザーがデータベース内のデータにアクセスしたり変更したりするために持つ許可または特権のことです。ユーザー権限は、レプリケーション中のデータベース競合の発生や解決に直接影響を与えるものではありません。ユーザー権限は、異なるデータベースにおけるユーザーの役割や機能によって異なる場合があり、各データベースのセキュリティポリシーと要件に従って定義および適用される必要があります。

最新問題: 248

以下の主要業績評価指標 (KPI) の変化のうち、システム可用性の低下を示すものはどれですか？

- A. 監視対象サービスの割合増加
- B. サービス復旧までの平均時間の増加
- C. ヘルプデスクの増員
- D. 故障間隔の平均時間の増加

Answer: B ([メッセージを残す](#))

最新問題: 249

An IS auditor has completed an audit of an organization's accounts payable system. Which of the following should be rated as the HIGHEST risk in the audit report and requires immediate remediation?

- A. Lack of segregation of duty controls for reconciliation of payment transactions
- B. Lack of segregation of duty controls for reversing payment transactions
- C. Lack of segregation of duty controls for removal of vendor records
- D. Lack of segregation of duty controls for updating the vendor master file

Answer: [\(解答を表示する\)](#)

最新問題: 250

組織が事業中断後も重要な事業運営を継続できる能力を検証する最も効果的な方法は次のうちどれですか？分析対象：

- A. エンドツーエンドの復旧フロー
- B. リカバリポイント目標 (RPO)
- C. コールツリー
- D. 事業影響分析 (BIA)

Answer: D ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 251

After initial investigation, an IS auditor has reasons to believe that fraud may be present.

The IS auditor should:

- A. expand activities to determine whether an investigation is warranted
- B. 監査委員会にこの件を報告する。
- C. 不正の可能性を経営陣に報告し、どのように対応したいか尋ねる。
- D. 外部の法律顧問に相談し、取るべき行動方針を決定する。

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

IS監査人の不正検出の責任には、不正の兆候を評価し、追加措置が必要かどうか、または調査を推奨すべきかどうか。IS監査担当者組織内の適切な当局に通知するのは、指標が不正行為の証拠は調査を勧告するのに十分である。通常、IS監査人は、外部の法律顧問に相談してください。

最新問題: 252

Which of the following is the MOST important consideration when developing an incident response program?

- A. Senior management support
- B. Technical skills of response staff
- C. Number of dedicated response staff
- D. Incident response procedures

Answer: A ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 253

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- A. Issue an audit finding
- B. Seek an explanation from IS management
- C. Review the classifications of data held on the server
- D. Expand the sample of logs reviewed

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

最新問題: 254

法医学目的でデジタルデータを収集する場合、イメージングの使用に伴う最大の利点は次のとおりである。

- A. 分析用に、元のデータと破損したファイルのビット単位のコピーを提供します。
- B. 研究者に効果的なデータ視覚化機能を提供する
- C. 残余スラックデータやフラグメントなどの不要なデータを再現しない
- D. フォレンジックデータの損失を防ぐためのリアルタイムディスクミラーリング機能を提供します

Answer: ([解答を表示する](#))

鑑識データ収集においてイメージングを用いる最大の利点は、破損したファイルも含め、元のデータのビット単位のコピーを提供できることであり、元の証拠を改変することなく、徹底的な分析のためにストレージメディアの正確な複製を確保できる点にある。

最新問題: 255

Which of the following is a rewrite of ipfwadm?

- A. ipchains
- B. iptables
- C. Netfilter
- D. ipcook
- E. None of the choices.

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is

superseded by iptables in Linux 2.4 and above. Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

最新問題: 256

Which of the following should be an IS auditor's PRIMARY focus when evaluating the response process for cyber crimes?

- A. Communication with law enforcement
- B. Notification to regulators
- C. Root cause analysis
- D. Evidence collection

Answer: D ([メッセージを残す](#))

According to the ISACA CISA Study Guide, the primary focus of an IS auditor when evaluating the response process for cyber crimes should be evidence collection. This is because the investigation and resolution of cyber incidents rely heavily on the evidence that is collected and analyzed. For more information, please refer to the ISACA CISA Study Guide section 4.13.2.2.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 257

経営陣に対し、ITに関する内部統制について利害関係者への報告書の発行を義務付けることの利点として、次のうちどれが挙げられますか？

- A. コスト管理の改善
- B. ポートフォリオ管理の改善
- C. ITガバナンスに注力
- D. ITコストの透明性

Answer: C ([メッセージを残す](#))

最新問題: 258

Which of the following is NOT an example of corrective control?

- A. OS Upgrade
- B. Backup and restore
- C. Contingency planning
- D. System Monitoring

Answer: D ([メッセージを残す](#))

Section: The process of Auditing Information System

Explanation:

The word NOT is used as a keyword in the question. You need to find out a security control from given

options which is not corrective control. System Monitoring is a detective control and not a corrective control. For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate

certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers.

Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In

addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples belong to corrective control.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

最新問題: 259

In a RAO model, which of the following roles must be assigned to only one individual?

- A.** Responsible
- B.** Informed
- C.** Consulted
- D.** Accountable

Answer: D ([メッセージを残す](#))

Explanation

In a RAO model, which stands for Responsible, Accountable, Consulted, and Informed, the accountable role must be assigned to only one individual. The accountable role is the person who has the ultimate authority and responsibility for the outcome of the project or task, and who approves or rejects the work done by the responsible role. The accountable role cannot be delegated or shared, as it is essential to have a clear and single point of accountability for each project or task.

The other roles can be assigned to more than one individual:

Responsible. This is the person who does the work or performs the task. There can be multiple responsible roles for different aspects or phases of a project or task, as long as they are coordinated and supervised by the accountable role.

Informed. This is the person who needs to be notified or updated about the progress or results of the project or task. There can be multiple informed roles who have an interest or stake in the project or task, but who do not need to be consulted or involved in the decision-making process.

Consulted. This is the person who provides input, feedback, or advice on the project or task. There can be multiple consulted roles who have expertise or experience relevant to the project or task, but who do not have the authority or responsibility to approve or reject the work done by the responsible role.

最新問題: 260

Which of the following is MOST important during software license audits?

- A.** Judgmental sampling
- B.** Substantive testing
- C.** Compliance testing
- D.** Stop-or-go sampling

Answer: B ([メッセージを残す](#))

Explanation

Substantive testing is the most important type of testing during software license audits, as it provides evidence of the accuracy and completeness of the software inventory and licensing records. Substantive testing involves examining transactions, balances, and other data to verify their validity, existence, accuracy, and valuation.

Compliance testing, on the other hand, is more focused on assessing the adequacy and effectiveness of internal controls over software licensing, such as policies, procedures, and monitoring mechanisms. Compliance testing alone cannot provide sufficient assurance that the software license audit objectives are met, as it does not verify the actual software usage and compliance

status. Judgmental sampling and stop-or-go sampling are methods of selecting samples for testing, not types of testing themselves. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 1206 Testing, "The IS audit and assurance professional should perform sufficient testing to obtain sufficient appropriate evidence to support conclusions reached." 1 The section also defines substantive testing as "testing performed to obtain audit evidence to detect material misstatements in transactions or balances" and compliance testing as "testing performed to obtain audit evidence on the operating effectiveness of controls." 1 According to the ISACA IT Audit and Assurance Guideline G15 Software License Management, "The objective of a software license audit is to provide management with an independent assessment relating to compliance with software license agreements." 2 The guideline also states that "substantive tests should be performed on a sample basis to verify that all software installed on devices within scope has been appropriately licensed." 2

最新問題: 261

After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

- A. Differential reporting
- B. False-positive reporting
- C. False-negative reporting
- D. Less-detail reporting

Answer: C ([メッセージを残す](#))

False-negative reporting on weaknesses means the control weaknesses in the network are not identified and therefore may not be addressed, leaving the network vulnerable to attack. False-positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

最新問題: 262

ITシステムの老朽化に関連する問題に最も効果的に対処できるのは、以下のうちどれでしょうか？

- A. ITプロジェクト管理
- B. リリース管理
- C. アプリケーションポートフォリオ管理
- D. 構成管理

Answer: B ([メッセージを残す](#))

セクション：情報システムの取得、開発、導入

最新問題: 263

The FIRST step in auditing a data communication system is to determine:

- A. traffic volumes and response-time criteria
- B. physical security for network equipment
- C. business use and types of messages to be transmitted
- D. the level of redundancy in the various communication paths

Answer: C ([メッセージを残す](#))

最新問題: 264

IS監査プログラムの洗練度と形式性は、
以下の要因？

- A. 対象企業の経営陣による直接的な関与。
- B. ターゲットの位置。
- C. ターゲットのサイズと複雑さ。
- D. 対象者の予算。
- E. 対象の人数。
- F. 選択肢に該当しない。

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

適切に計画されたリスクベースの監査プログラムは、監査の効率性と有効性を向上させる。
この種の監査の高度さや形式は、対象企業の規模や複雑さによって大きく異なる。

最新問題: 265

Which of the following is the MAIN benefit of using data analytics when testing the effectiveness of controls?

- A. Analytics remove the need to focus on areas of higher risk
- B. The full population can be tested.
- C. The demand for IS auditors is reduced over time
- D. Analytics can be applied to any type of control

Answer: B ([メッセージを残す](#))

最新問題: 266

Which of the following provides an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately?

- A. Electronic copies of customer sales receipts are maintained.
- B. Monthly bank statements are reconciled without exception.
- C. Nightly batch processing has been replaced with real-time processing.
- D. The data transferred over the POS interface is encrypted.

Answer: A ([メッセージを残す](#))

Explanation

The best option to provide an IS auditor assurance that the interface between a point-of-sale (POS) system and the general ledger is transferring sales data completely and accurately is A. Electronic copies of customer sales receipts are maintained. Electronic copies of customer sales receipts are records of the transactions that occurred at the POS system, which can be compared with the data transferred to the general ledger. This can help detect any errors, omissions, or discrepancies in the data transfer process and ensure that the sales data is complete and accurate.

The other options are not as effective as A in providing assurance that the interface between the POS system and the general ledger is transferring sales data completely and accurately. B. Monthly bank statements are reconciled without exception.

Monthly bank statements are records of the cash inflows and outflows of the organization, which may not match with the sales

data recorded by the POS system and the general ledger. For example, there may be delays, discounts, returns, or refunds that affect the cash flow but not the sales revenue.

Therefore, reconciling monthly bank statements without exception does not necessarily mean that the sales data is complete and accurate. C. Nightly batch processing has been replaced with real-time processing.

Nightly batch processing is a method of transferring data from the POS system to the general ledger in batches at a scheduled time, usually at night. Real-time processing is a method of transferring data from the POS system to the general ledger as soon as the transactions occur. Real-time processing may improve the timeliness and efficiency of the data transfer process, but it does not guarantee that the sales data is complete and accurate. There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected. D. The data transferred over the POS interface is encrypted.

Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access the original data. Encryption protects the confidentiality and security of the data transferred over the POS interface, but it does not ensure that the sales data is complete and accurate. There may still be errors, omissions, or discrepancies in the data transfer process that need to be detected and corrected.

References:

ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471

ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2 Sales Audit Overview - Oracle3

Notes on Audit of Ledgers - Guidelines to Auditors - Accountlearning

最新問題: 267

Which of the following concerns is BEST addressed by defining job dependencies when creating job schedules?

- A. The jobs rely on manual data preparation
- B. Job failure notifications are not sent in a timely manner
- C. Subsequent jobs rely on unprocessed information
- D. Subsequent jobs require additional approvals

Answer: (解答を表示する)

Defining job dependencies ensures that jobs are executed in the correct sequence, meaning subsequent jobs will not begin until the preceding jobs have successfully completed and provided the necessary data. This prevents situations where jobs that rely on unprocessed or incomplete information are triggered prematurely, which could lead to errors and data inconsistencies.

While manual data preparation, failure notifications, and additional approvals are important, job dependencies primarily address the sequencing and flow of jobs to ensure that dependent processes run only after the necessary preconditions are met.

最新問題: 268

An organization's IT department and internal IS audit function all report to the chief information officer (CIO). Which of the following is the GREATEST concern associated with this reporting structure?

- A. Potential for inaccurate audit findings
- B. Compromise of IS audit independence
- C. IS audit resources being shared with other IT functions
- D. IS audit being isolated from other audit functions

Answer: B (メッセージを残す)

The greatest concern with the IT department and internal IS audit function both reporting to the CIO is the potential compromise of IS audit independence. Auditor independence refers to the impartiality and objectivity of an auditor in conducting an audit, free

from conflicts of interest and bias¹. It is crucial for ensuring the quality and reliability of financial reporting¹. If the IS audit function reports to the CIO, who also oversees the IT department, it could create a conflict of interest that might compromise the impartiality and objectivity of the IS audit function.

References:

Auditor Independence - What is it, Rules, Importance, Examples

最新問題: 269

When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

- A. node list.
- B. acceptance test report.
- C. network diagram.
- D. user's list.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

To properly review a LAN implementation, an IS auditor should first verify the network diagram and confirm the approval.

Verification of nodes from the node list and the network diagram would be next, followed by a review of the acceptance test report and then the user's list.

最新問題: 270

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- A. True
- B. False

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Database snapshots can provide an excellent audit trail for an IS auditor.

最新問題: 271

A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?

- A. Audit logs are not enabled for the system
- B. A logon ID for the technical lead still exists
- C. Spyware is installed on the system
- D. A Trojan is installed on the system

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Audit logs are critical to the investigation of the event; however, if not enabled, misuse of the logon ID of the technical lead and the guest account could not be established. The logon ID of the technical lead should have been deleted as soon as the

employee left the organization but, without audit logs, misuse of the ID is difficult to prove. Spyware installed on the system is a concern but could have been installed by any user and, again, without the presence of logs, discovering who installed the spyware is difficult. A Trojan installed on the system is a concern, but it can be done by any user as it is accessible to the whole group and, without the presence of logs, investigation would be difficult.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **272**

Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

- A. Developments may result in hardware and software incompatibility.
- B. Resources may not be available when needed.
- C. The recovery plan cannot be tested.
- D. The security infrastructures in each company may be different.

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based walkthroughs, and possibly by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

最新問題: **273**

組織の情報システムの目的を説明する上で、次のうちどれが最適な情報源ですか？

- A. ビジネスプロセスオーナー
- B. エンドユーザー
- C. IT管理
- D. 情報セキュリティ管理

Answer: D ([メッセージを残す](#))

セクション :ITのガバナンスと管理

説明／参考資料：

最新問題: **274**

組織のシステムが分散型サービス拒否 (DDoS) 攻撃に参加するのを防ぐのに役立つのは、次のうちどれですか？最適な回答を選択してください。

- A. 受信トラフィックのフィルタリング
- B. アクセス制御リスト (ACL) を使用して、受信接続試行を制限する
- C. 送信トラフィックのフィルタリング
- D. 分散システムの再集中化

Answer: C ([メッセージを残す](#))

説明／参考資料：

送信トラフィックのフィルタリングは、組織のシステムが分散型サービス拒否 (DDoS) 攻撃に
関与するのを防ぐのに役立ちます。

最新問題: 275

内部監査機能において内部品質保証 (QA) を実施する主な理由は、以下の点を確実にすることです。

- A. 監査リソースが最も効果的に活用されます。
- B. 内部監査活動は監査基準および方法論に準拠している。
- C. 監査機能は適切に管理されており、パフォーマンス指標を満たしている。
- D. 監査における固有リスクが最小限に抑えられます。

Answer: B ([メッセージを残す](#))

内部監査機能において内部品質保証 (QA) を実施する主な理由は、内部監査活動が、内部監査人協会 (IIA) が発行する「内部監査の定義」および「内部監査の専門的実務に関する国際基準」(基準ならびに組織の内部監査方法論および方針に準拠していることを確認するためです。QAプログラムは、内部監査活動のパフォーマンス、効率性、有効性、および価値を評価し、改善の機会を特定することを可能にします。また、QAプログラムは、ステークホルダーの間での内部監査機能の信頼性と評判を高めることにも役立ちます。

参考文献

品質保証 - 内部監査人協会 (IIA)

内部監査における品質保証レビューの利点

品質保証レビューで内部監査機能を最適化しましょう...

最新問題: 276

An IS audit team is evaluating documentation of the most recent application user access review. It is determined that the user list was not system generated. Which of the following should be of MOST concern?

- A. Confidentiality of the user list
- B. Completeness of the user list
- C. Timeliness of the user list review
- D. Availability of the user list

Answer: B ([メッセージを残す](#))

最新問題: 277

Which of the following is the BEST testing approach to facilitate rapid identification of application interface errors?

- A. Automated testing
- B. User acceptance testing (UAT)

C. Regression testing

D. Integration testing

Answer: A ([メッセージを残す](#))

最新問題: 278

Which of the following should be of GREATEST concern for an IS auditor when reviewing user account policies?

A. 退職時に従業員のシステムアクセス権を取り消す方針はありません。

B. 継続的なセキュリティ意識向上トレーニングに関する方針は存在しません。

C. 従業員に秘密保持契約 (NDA) への署名を義務付ける方針はありません。

D. 従業員が役割を変更した場合でも、以前のアクセス権限を取り消すポリシーはありません。

Answer: A ([メッセージを残す](#))

退職時にアクセス権を取り消さなかった場合、元従業員が機密データやシステムにアクセスできる可能性があるため、最大のセキュリティリスクとなる。

アクセス権を取り消すポリシーはありません（正解 A）

解雇された従業員がアクセス権を保持している場合、データ漏洩や内部脅威につながる可能性がある。

例：元従業員が、現在使用している認証情報を悪用して金融システムにアクセスする。

セキュリティ意識向上トレーニングの不足（不正解 B）

重要ではあるが、アクティブな元従業員アカウントのように、差し迫ったセキュリティリスクをもたらすものではない。

秘密保持契約なし（誤り - C）

知的財産を保護するが、システムアクセスほど重要ではない。

役割変更に対するアクセス権の取り消しは行われたい（誤り - D）

依然として懸念事項ではあるが、現在もアクセス権限を持つ元従業員はより高いリスクを伴う。

参考文献：

ISACA CISAレビューマニュアル

NIST 800-53 アクセス制御

最新問題: 279

The PRIMARY benefit of a risk-based audit methodology is to:

A. prioritize audit resources.

B. reduce audit scope.

C. understand business processes.

D. identify key controls.

Answer: C ([メッセージを残す](#))

最新問題: 280

What should IS auditors always check when auditing password files?

A. That deleting password files is protected

B. That password files are encrypted

C. That password files are not accessible over the network

D. That password files are archived

Answer: B ([メッセージを残す](#))

Explanation/Reference:

IS auditors should always check to ensure that password files are encrypted.

最新問題: 281

An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

- A. False-acceptance rate (FAR)
- B. Equal-error rate (EER)
- C. False-rejection rate (FRR)
- D. False-identification rate (FIR)

Answer: ([解答を表示する](#)**)**

FAR is the frequency of accepting an unauthorized person as authorized, thereby granting access when it should be denied, in an organization with high security requirements, user annoyance with a higher FRR is less important, since it is better to deny access to an authorized individual than to grant access to an unauthorized individual. EER is the point where the FAR equals the FRR; therefore, it does not minimize the FAR. FIR is the probability that an authorized person is identified, but is assigned a false ID.

最新問題: 282

ウェブサイトの認証に使用され、データ暗号化に使用される鍵の認証にも使用できるものは何ですか？

- A. 組織証明書
- B. ユーザー証明書
- C. ウェブサイト証明書
- D. オーセンティックコード

Answer: C ([メッセージを残す](#))

説明／参考資料：

ウェブサイト証明書は、ウェブサイトの認証を行うために使用され、データ暗号化に使用される鍵の認証にも使用できます。

最新問題: 283

ある組織は、サポート終了となったデータベースを一元的に廃止し、データを最新のハードウェアモデルに移行する計画を立てています。移行中にデータの整合性を最も確実に維持できる方法は次のうちどれですか？

- A. サンプルデータを最新のバックアップデータと照合する
- B. 機密データの難読化
- C. データの暗号化
- D. チェックサムの比較

Answer: D ([メッセージを残す](#))

最新問題: 284

組織のISセキュリティポリシーには、次のうちどれを含めるべきでしょうか？

- A. 確保すべき主要なITリソースのリスト

- B. アクセス権限の根拠
- C. 機密性の高いセキュリティ機能の識別
- D. 関連するソフトウェアセキュリティ機能

Answer: B ([メッセージを残す](#))

セキュリティポリシーは、上級管理職によって策定・承認された、セキュリティに関する大まかな枠組みを提供するものです。アクセス権限を持つ者の定義と、アクセス権限付与の根拠が含まれています。選択肢A、B、Cは、ポリシーに含めるべき内容よりも詳細です。

最新問題: 285

他のほとんどすべての懸念事項の中でも、新しいアプリケーションソフトウェアの導入に最も大きな悪影響を与えるものは何でしょうか？

- A. ユーザー受け入れテストの実施に失敗した
- B. 新システムに関するユーザー研修の不足
- C. ソフトウェアのドキュメントと実行マニュアルが不足している
- D. ユニット、モジュール、およびシステムのテストが不十分

Answer: A ([メッセージを残す](#))

他のほとんどすべての懸念事項の中でも、ユーザー受け入れテストを実施しないことは、新しいアプリケーションソフトウェアの導入に最も大きな悪影響を与えることが多い。

最新問題: 286

.What should IS auditors always check when auditing password files?

- A. That deleting password files is protected
- B. That password files are encrypted
- C. That password files are not accessible over the network
- D. That password files are archived

Answer: B ([メッセージを残す](#))

IS auditors should always check to ensure that password files are encrypted.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 287

IS監査人が、ある会社の幹部が従業員にソーシャルネットワーキングサイトの使用を奨励していることを発見した。

ビジネス目的。以下の推奨事項のうち、データリスクを軽減するのに最も役立つのはどれですか。

漏れ？

- A. 従業員による方針確認書および秘密保持契約書の署名を義務付ける

- B. 従業員に対し、ソーシャルネットワーキングサイトの利用に関する教育とガイドラインを提供する。
- C. 機密データに対する強力なアクセス制御の確立
- D. 従業員のソーシャルネットワーク利用状況の監視

Answer: B ([メッセージを残す](#))

セクション :ITのガバナンスと管理

最新問題: 288

デジタル著作権管理 (DRM) アプリケーションをレビューするIS監査担当者は、以下のどの技術が広く使用されていると予想すべきでしょうか？

- A. デジタル署名
- B. ハッシュ化
- C. 構文解析
- D. ステガノグラフィー

Answer: D ([メッセージを残す](#))

セクション : 情報資産の保護

Explanation:

ステガノグラフィーは、メッセージや情報の存在を隠蔽する技術です。ますます重要になっているステガノグラフィー技術はデジタル透かしで、これは、画像や音楽の知覚可能な美的特性を変えことなく、著作権情報を画像や音楽ファイルにエンコードするなどして、データの中にデータを隠します。デジタル署名は、デジタル著作権管理とは関係ありません。ハッシュ化はメッセージのハッシュまたはダイジェストを作成し、メッセージの完全性を保証するために使用されます。これは通常、暗号化の一部とみなされます。パースは、分析目的で連続した文字ストリームを分割するプロセスであり、プログラミング言語の設計やデータ入力編集に広く適用されています。

最新問題: 289

IT投資がビジネス目標を達成しているかどうかを評価する際に、IS監査担当者にとって最も有用な指標は次のうちどれですか？

- A. 予算支出と実際の支出の比較
- B. 実際の顧客満足度と予測される顧客満足度の比較
- C. 実際の投資収益率 (ROI) と業界平均ROIの比較。
- D. 実現投資収益率 (ROI) と予測投資収益率の比較

Answer: ([解答を表示する](#)**)**

最新問題: 290

情報システム監査担当者が、インターネットに接続された重要なシステムが攻撃に対して脆弱であり、パッチが提供されていないことを発見しました。監査担当者は、まず何を行うよう推奨すべきでしょうか？

- A. パッチ適用可能な新しいシステムを導入する。
- B. システムを保護するために追加のファイアウォールを導入してください。
- C. 関連するリスクを評価する。
- D. サーバーを停止します。

Answer: C ([メッセージを残す](#))

最新問題: 291

Which of the following key performance indicators (KPIs) provides stakeholders with the MOST useful information about whether information security risk is being managed?

- A. Time from identifying security threats to implementing solutions
- B. The number of security controls audited
- C. Time from security log capture to log analysis
- D. The number of entries in the security risk register

Answer: ([解答を表示する](#))

The speed at which security threats are mitigated is a key indicator of an organization's risk management effectiveness.

Option A (Correct): Response time to security threats measures how efficiently security teams detect, analyze, and mitigate risks, providing clear insight into security operations.

Option B (Incorrect): The number of security controls audited does not indicate how well risk is being managed, only that reviews are taking place.

Option C (Incorrect): Log analysis speed is useful, but it does not directly measure risk mitigation effectiveness.

Option D (Incorrect): Risk register entries indicate known risks but do not provide insight into how well those risks are managed.

Reference: ISACA CISA Review Manual -Domain 5: Protection of Information Assets- Covers security metrics, KPIs, and risk management evaluation.

最新問題: 292

チェックデジットは、以下の項目に対する効果的な編集チェックです。

- A. データ転記エラーを検出する
- B. データ転置エラーと転写エラーを検出する
- C. データの転置、転写、置換エラーを検出します
- D. データ転置エラーを検出する

Answer: ([解答を表示する](#))

チェックデジットは、データの転記ミスや書き間違いを検出するための効果的な編集チェック手段です。

最新問題: 293

Which of the following would have the GREATEST impact on defining the classification levels for electronic documents?

- A. Value of information
- B. Volume of information
- C. Document archival requirements
- D. End user preferences

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

最新問題: 294

監査目標を設定する際の主要な根拠となるのは、次のうちどれですか？

- A. ビジネス戦略
- B. 監査リスク

C. リスクの検討

D. 過去の監査の評価

Answer: A ([メッセージを残す](#))

最新問題: 295

次のうち、電子メールのフォーマットをあるネットワークから別のネットワークに変換して、メッセージがすべてのネットワークを通過できるようにするものはどれですか？

A. ゲートウェイ

B. プロトコルコンバータ

C. フロントエンド通信プロセッサ

D. コンセントレータ／マルチプレクサ

Answer: ([解答を表示する](#))

ゲートウェイは、電子メールのフォーマットをあるネットワークから別のネットワークに変換する役割を果たします。

メッセージはあらゆるネットワークを経由して伝達される可能性がある。

不正解：

B. プロトコルコンバータは、非同期伝送と同期伝送など、2種類の異なる伝送方式を相互に変換するハードウェア デバイスです。

C. フロントエンド通信プロセッサは、すべてのネットワーク通信回線を中央コンピュータに接続し、中央コンピュータがネットワーク制御、フォーマット変換、メッセージ処理などのタスクを実行する負担を軽減します。

D. コンセントレータ/マルチプレクサは、複数の低速チャネルを高速チャネルに結合するために使用されるデバイスです。

最新問題: 296

インターネットからの攻撃経路が最小限に抑えられていることを確認するために組織のネットワークを監査するIS監査担当者は、次のうちどれを懸念すべきでしょうか？

A. 組織のファイアウォールの内側にデータ損失防止 (DLP) システムがあります。

B. ルーターはネットワーク境界でインターネットに接続されています。

C. 組織のメールサーバーは非武装地帯 (DMZ) にあります。

D. 組織は非武装地帯 (DMZ) で様々な種類のファイアウォールを採用しています。

Answer: B ([メッセージを残す](#))

最新問題: 297

During an audit of a payroll system, an IS auditor identifies that two employees share the same bank account. The auditor is concerned they may be ghost employees. Which of the following should the auditor do NEXT?

A. Notify the human resources executive immediately.

B. Advise payroll management to suspend both employees accounts until further investigated.

C. Conduct inquiries to determine whether the two employees have a relationship.

D. Draft a report with a finding that there may be ghost employees.

Answer: C ([メッセージを残す](#))

最新問題: 298

Which of the following should an IS auditor be MOST concerned with during a post-implementation review?

- A. The system does not have a maintenance plan.
- B. The system contains several minor defects.
- C. The system deployment was delayed by three weeks.
- D. The system was over budget by 15%.

Answer: A ([メッセージを残す](#))

Explanation

A post-implementation review (PIR) is an assessment conducted at the end of a project cycle to determine if the project was indeed successful and to identify any existing flaws in the project¹. One of the main objectives of a PIR is to evaluate the outcome and functional value of a project¹. Therefore, an IS auditor should be most concerned with whether the system meets the intended requirements and delivers the expected benefits to the stakeholders. A system that does not have a maintenance plan is a major risk, as it may not be able to cope with changing needs, fix errors, or prevent security breaches. A maintenance plan is essential for ensuring the system's reliability, availability, and performance in the long term².

The other options are less critical for a PIR, as they are more related to the project management aspects than the system quality aspects. The system may contain several minor defects that do not affect its functionality or usability, and these can be resolved in future updates. The system deployment may be delayed by three weeks due to unforeseen circumstances or dependencies, but this does not necessarily mean that the system is faulty or ineffective. The system may be over budget by 15% due to various factors such as scope creep, resource constraints, or market fluctuations, but this does not imply that the system is not valuable or beneficial.

References: 1: Post-Implementation Review Best Practices - MetaPM 2: What is Post-Implementation Review in Project Management?

最新問題: 299

進行中のサービス拒否 (DoS) 攻撃に対応する際、組織が最初にとるべき行動は

- A. サービスを復旧する
- B. 損傷を調査する
- C. 攻撃経路の分析
- D. 影響を最小限に抑える

Answer: D ([メッセージを残す](#))

最新問題: 300

組織のITガバナンスを導くためにフレームワークを使用することの最大の利点は次のうちどれですか？

- A. IT部門と実際のビジネス部門間のサービスレベルの達成を可能にします。
- B. 組織全体で戦略的なIT投資を行う際に、一貫性を保つことができます。
- C. 組織内の高リスクシステムのセキュリティを向上させることができます。
- D. 取締役会から提供される年間IT予算のより良い管理を可能にします。

Answer: B ([メッセージを残す](#))

最新問題: 301

技術の変化の速度は、以下の重要性を高めます。

- A. IS機能を外部委託する。
- B. 適切なプロセスを導入し、徹底する。
- C. 組織内でキャリアを築きたいと考えている人材を採用します。
- D. ユーザーの要求を満たす。

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

変化に対応するには、適切な変更管理プロセスを導入し、徹底する必要があります。情報システム (IS) 機能のアウトソーシングは、技術変化の速度とは直接関係がありません。一般的なIS部門の従業員は高度な資格と教育を受けており、通常は自分の仕事が危ういとは感じておらず、頻繁に転職する用意があります。ユーザー要件を満たすことは重要ですが、IS環境における技術変化の速度とは直接関係がありません。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **302**

ある企業では、すべてのプログラム変更要求 (PCR) が承認され、すべての変更が自動的に記録されることが求められています。本番プログラムに不正な変更が加えられたかどうかを最も適切に判断できる情報システム監査手順は次のうちどれでしょうか？

- A. 完全なPCRフォームのサンプルを、すべてのプログラム変更のログにトレースする
- B. ソースコード比較ソフトウェアを使用して、前回の監査日以降にサンプルプログラムに変更が加えられたかどうかを判定する。
- C. プログラム変更プロセス全体を通して、PCRのサンプルをレビューし、適切な承認を得る。
- D. プログラム変更のサンプルをログから完成したPCRフォームまで追跡する

Answer: ([解答を表示する](#)**)**

説明

The best way to determine whether unauthorized changes have been made to production programs is to use source code comparison software to compare the current version of the programs with the previous version or the approved version. This will identify any changes that have been made without proper authorization or documentation. Tracing PCR to logs or vice versa will only verify that the authorized changes have been recorded, but not detect any unauthorized changes. References: Standards, Guidelines, Tools and Techniques - ISACA, section "IS Audit and Assurance Tools and Techniques"

最新問題: **303**

自社開発アプリケーションを本番環境で侵入テストする際に、最も懸念される点は次のうちどれですか？

- A. このテストでは、既知のオペレーティングシステムの脆弱性のみを特定できる場合があります。
- B. テストによってアプリケーションの可用性に問題が生じる可能性があります。
- C. テスト中に特定された問題には、相当な修復作業が必要となる可能性があります。

D. 内部セキュリティ担当者は、アプリケーションの侵入テストを実施する資格がない可能性があります。

Answer: B ([メッセージを残す](#))

最新問題: 304

社内ヘルプデスクの手順がポリシーに準拠して実行されていることを確認するための最適な方法は、次のうちどれですか？

- A. ヘルプデスクの手順をベンチマークする。
- B. エンドユーザーにインタビューする。
- C. クローズされたチケットのサンプルをテストします。
- D. ヘルプデスクの通話指標を評価する。

Answer: C ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 305

An IS auditor discovers a box of hard drives in a secured location that are overdue for physical destruction.

The vendor responsible for this task was never made aware of these hard drives. Which of the following is the BEST course of action to address this issue?

- A. Examine the workflow to identify gaps in asset handling responsibilities.
- B. Recommend the drives be sent to the vendor for destruction.
- C. Escalate the finding to the asset owner for remediation
- D. Evaluate the corporate asset handling policy for potential gaps.

Answer: ([解答を表示する](#))

最新問題: 306

Which of the following is the MOST effective type of antivirus software?

- A. Scanners
- B. Active monitors
- C. integrity checkers
- D. Vaccines

Answer: ([解答を表示する](#))

Section: Protection of Information Assets

Explanation:

整合性チェッカーは、既知のウイルスフリーのプログラムに対してバイナリ数を計算し、それをデータベース ファイル。この番号は巡回冗長検査 (CRC) と呼ばれます。そのプログラムが呼び出されると実行時に、チェッカーは実行しようとしているプログラムのCRCを計算し、それをデータベース内の番号。一致は感染なしを意味し、不一致はプログラムの変更を意味します。発生しました。プログラムの変更はウイルス感染の可能性があります。スキャナーは、ビット列を探します。ウイルスプログラムに典型的なシグネチャ。メモリ、ディスクブートセクタ、実行ファイル、既知のウイルスと一致するビットパターンに対応するコマンドファイル。そのため、スキャナーを更新する必要があります。定期的に有効性を維持する。アクティブモニタは、DOSおよびROM基本入出力システム (BIOS) を解釈する。ウイルスのような動作を探すための呼び出し。

アクティブモニターは、ユーザー要求とプログラムの動作を区別できないため、誤解を招く可能性があります。
またはウイルス要求。結果として、ユーザーはディスクのフォーマットやファイルの削除などの操作を確認するように求められます。
一連のファイル。ワクチンは優れたウイルス対策ソフトとして知られています。しかし、ワクチンもアップデートが必要です。
効果を維持するためには定期的に行う必要がある。

最新問題: 307

以下の活動のうち、組織内に存在する可能性のある個人間の依存関係について、IS監査担当者に最も深い洞察を与えるのはどれですか？

- A. ユーザーアクティビティログの確認
- B. ITプロセスを役割にマッピングする
- C. 休暇パターンの見直し
- D. IT部門の上級管理職へのインタビュー

Answer: B ([メッセージを残す](#))

最新問題: 308

新しいアプリケーションシステムの導入中にデータ変換と移行をレビューする監査担当者にとって、次のうちどれが最も懸念すべき事項でしょうか？

- A. 変更管理プロセスが正式に文書化されていませんでした
- B. 旧システムおよびデータのバックアップはオンラインでは利用できません
- C. 変換中に不正なデータ変更が発生しました。
- D. データ変換は手動プロセスを使用して実行されました。

Answer: C ([メッセージを残す](#))

説明

新しいアプリケーションシステムの導入中にデータ変換と移行をレビューするIS監査担当者にとって最も懸念すべき点は、変換中に不正なデータ変更が発生したことです。データ変換と移行とは、あるシステムから別のシステムにデータを転送し、その正確性、完全性、整合性、および使いやすさを確保するプロセスです。変換中の不正なデータ変更は、データの損失、破損、不整合、または重複を引き起こし、新しいシステムの機能性、パフォーマンス、信頼性、およびセキュリティに影響を与える可能性があります。また、不正なデータ変更は、意思決定、レポート作成、コンプライアンス、顧客サービス、および収益に影響を与えるなど、ビジネスに重大な影響を及ぼす可能性もあります。IS監査担当者は、アクセス制御、データ検証、照合、監査証跡、バックアップとリカバリなど、変換中の不正なデータ変更を防止、検出、および修正するための適切な制御が整備されていることを確認する必要があります。その他の所見 A、B、およびD)は、変更管理プロセスを文書化したり、旧システムのバックアップとデータをオフラインストレージから復元したり、データ変換プロセスを自動化したりすることで軽減できるため、それほど懸念する必要はありません。参考文献 :CISAレビューマニュアル (デジタル版)、第3章：情報システムの取得、開発、実装、第3.4節 :システムの実装

最新問題: 309

Which of the following is MOST important for an IS auditor to ensure is included in a global organization's online data privacy notification to customers?

- A. Consequences to the organization for mishandling the data
- B. Consent terms including the purpose of data collection

C. Contact information for reporting violations of consent

D. Industry standards for data breach notification

Answer: B ([メッセージを残す](#))

Section: The process of Auditing Information System

最新問題: 310

内部監査チームは、別の国にある第三者がホストする監査管理アプリケーションを使用するかどうかを検討している。ホスト型アプリケーションへの給与監査関連書類のアップロードに関して、最も重要な考慮事項は何でしょうか？

A. 組織に影響を与える財務規制

B. アプリケーションがホストされているデータセンターの物理アクセス制御

C. 組織に影響を与えるプライバシー規制

D. ホスティングサービスプロバイダーがストレージに対して請求する単位あたりの料金

Answer: ([解答を表示する](#)**)**

これは、プライバシー規制が、個人の個人情報を第三者による不正アクセス、使用、開示、または転送から保護する法律または規則であるためです。給与監査文書には、従業員の氏名、給与、福利厚生、税金、控除、銀行口座などの機密データや秘密情報が含まれる場合があります。監査管理アプリケーションが別の国の第三者によってホストされている場合、組織は自国とホスト国の両方のプライバシー規制、および適用される国際的または地域的な協定や枠組みを遵守する必要がある場合があります。プライバシー規制は、データ主体からの同意の取得、適切なセキュリティ対策の実施、データ侵害の通知、データの品質と正確性の確保など、組織にさまざまな要件と義務を課す場合があります。

プライバシー規制は、データ主体に対し、データへのアクセス、訂正、削除、転送など、さまざまな権利を付与する場合もあります。プライバシー規制を遵守しない場合、組織は訴訟、罰金、制裁、評判の低下、信頼の喪失など、重大なリスクと結果に直面する可能性があります。

組織に影響を与えるプライバシー規制の例としては、以下のようなものがあります。

* 一般データ保護規則 (GDPR)は、組織やデータの所在地に関係なく、欧州連合 (EU) 内の個人の個人データを処理する組織、または個人に商品やサービスを提供する組織に適用される包括的かつ厳格なプライバシー規制です1。

* カリフォルニア州消費者プライバシー法 (CCPA)は、カリフォルニア州居住者の個人情報を収集し、一定の収益、データ量、またはデータ共有の基準を満たすすべての組織に適用される、広範かつ影響力のあるプライバシー規制です2。

* 医療保険の携行性と説明責任に関する法律 (HIPAA)は、医療提供者、医療保険プラン、医療クリアリングハウスなど、米国の個人の保護対象医療情報 (PHI) を扱うあらゆる組織に適用される、分野別のプライバシー規制です3。

したがって、異なる国にある第三者がホストする監査管理アプリケーションを使用する前に、内部監査チームは、組織に影響を与えるプライバシー規制を徹底的に評価し、それらを遵守するための適切なポリシー、手順、および管理体制が整っていることを確認する必要があります。

最新問題: 311

重要なソフトウェアアプリケーションを交換する際、ビジネスプロセスの中断リスクが最も低いのは次のうちどれですか？

A. 並列実装

B. パイロット実施

C. 段階的実装

D. ビッグバン実装

Answer: ([解答を表示する](#)**)**

セクション：情報システムの運用、保守およびサポート

最新問題: 312

ITプロジェクトに事業継続計画（BCP）を組み込むことで、以下のメリットが得られます。

- A. 事業継続要件の改修。
- B. より包括的な要件セットの開発。
- C. トランザクションフローチャートの作成。
- D. アプリケーションがユーザーのニーズを満たすことを保証する。

Answer: (解答を表示する)

セクション：情報資産の保護

Explanation:

事業継続計画（BCP）を開発プロセスに組み込むことで、完全な網羅性を確保できます。

プロジェクトの各フェーズにおける要件。事業継続計画の改修

要件は、BCPが開発方法論に統合されていない場合に発生します。

フローチャートはアプリケーションの制御を分析するのに役立ちます。事業継続計画は直接的にユーザーの詳細な処理ニーズ。

最新問題: 313

母集団全体を選択することが現実的でない状況において、適切なサンプルサイズを決定する際に、情報システム監査担当者が最も考慮すべき事項は次のうちどれですか？

- A. 許容誤差
- B. データのアクセス可能性
- C. データ整合性
- D. 被監査者の対応力

Answer: A (メッセージを残す)

セクション：情報システムの監査プロセス

最新問題: 314

ある組織のIT部門は、物理サーバーの数を削減するために大規模な仮想化プロジェクトに着手している。

フットプリント。情報セキュリティマネージャーにとって、次のうちどれが最も優先順位が高いでしょうか？

- A. インシデントの管理方法を決定する
- B. 仮想化ソフトウェアの選択
- C. プロジェクトの設計段階から関わる
- D. プロジェクトに適切な安全資金が確保されていることを確認する

Answer: C (メッセージを残す)

セクション：ITのガバナンスと管理

最新問題: 315

次のうち、ネットワークフィルタが機能していることを示す証拠となるものはどれですか？

D18912E1457D5D1DDCBD40AB3BF70D5D

- A. ネットワークポートスキャンを実行する
- B. ネットワークパフォーマンスの分析
- C. ネットワークフィルタリングポリシーの見直し
- D. ネットワーク構成ルールの確認

Answer: A ([メッセージを残す](#))

最新問題: 316

The MOST effective biometric control system is the one:

- A. which has the highest equal-error rate (EER).
- B. which has the lowest EER.
- C. for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- D. for which the FRR is equal to the failure-to-enroll rate (FER).

Answer: B ([メッセージを残す](#))

Explanation/Reference:

Explanation:

The equal-error rate (EER) of a biometric system denotes the percent at which the false-acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfumps**)

最新問題: 317

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

- A. With public-key encryption, or symmetric encryption
- B. With public-key encryption, or asymmetric encryption
- C. With shared-key encryption, or symmetric encryption
- D. With shared-key encryption, or asymmetric encryption

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

最新問題: 318

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

- A. comply with regulatory requirements.
- B. provide a basis for drawing reasonable conclusions.
- C. ensure complete audit coverage.
- D. perform the audit according to the defined scope.

Answer: B ([メッセージを残す](#))

Explanation/Reference:

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them.

Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

最新問題: 319

What influences decisions regarding criticality of assets?

- A. The business criticality of the data to be protected
- B. Internal corporate politics
- C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
- D. The business impact analysis

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

最新問題: 320

複数の多様なサブシステムを持つリモートアクセスネットワークにおいて、以下の制御のうちどれが最も包括的でしょうか？

- A. プロキシサーバー
- B. ファイアウォールのインストール
- C. ネットワーク管理者
- D. パスワードの実装と管理

Answer: D ([メッセージを残す](#))

この状況において最も包括的な対策は、パスワードの実装と管理です。ファイアウォールは主要な防御手段ですが、すべてのアクセスを保護できるわけではないため、一定のリスクが残ります。プロキシサーバーはファイアウォールの一種であるため、同じルールが適用されます。ネットワーク管理者も対策の一つとして機能しますが、通常、複数の多様なシステムに対しては十分な対策とは言えません。

最新問題: 321

組織の事業継続計画をレビューしていた情報システム監査担当者は、組織のデータファイルとソフトウェアファイルが定期的にバックアップされていることを確認しました。これは、効果的な計画のどのような特徴を示しているのでしょうか？

- A. 抑止力
- B. 緩和
- C. 回復
- D. 応答

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

効果的な事業継続計画には、災害の影響を軽減するための対策が含まれます。バックアップ計画を効果的に機能させるには、ファイルを迅速に復元する必要があります。抑止策の一例として、情報システムにファイアウォールを設置することが挙げられます。復旧策の一例として、通常の業務を再開するためのホットサイトを組織内に設けることが挙げられます。

最新問題: **322**

Which of the following is the GREATEST risk of cloud computing?

- A. Lack of scalability
- B. Reduced performance
- C. Inflexibility
- D. Disclosure of data

Answer: C ([メッセージを残す](#))

最新問題: **323**

以下のうち、IT部門と企業ミッションの整合性を最もよく示しているのはどれですか？

- A. 年次取締役会
- B. IT部門の機能分析
- C. 四半期ごとの運営委員会会議
- D. 上級管理職への隔週報告

Answer: ([解答を表示する](#))

最新問題: **324**

Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

- A. Project segments are established.
- B. The work is separated into phases.
- C. The work is separated into sprints.
- D. Project milestones are created.

Answer: C ([メッセージを残す](#))

The best way to enable the effectiveness of an agile project for the rapid development of a new software application is to separate the work into sprints. Sprints are short, time-boxed iterations that deliver a potentially releasable product increment at the end of each sprint. Sprints allow agile teams to work in a flexible and adaptive manner, respond quickly to changing customer

needs and feedback, and deliver value faster and more frequently. Sprints also help teams to plan, execute, review, and improve their work in a collaborative and transparent way. Project segments, phases, and milestones are not specific to agile projects and do not necessarily enable the effectiveness of an agile project. References: Agile Project Management [What is it & How to Start] - Atlassian, CISA Review Manual (Digital Version).

最新問題: 325

高温、温暖、低温のサイトとの契約において、契約条項には以下のうちどれを規定すべきか。
考慮事項は？

- A. 物理的なセキュリティ対策
- B. 加入者総数
- C. サイトを同時に利用できる加入者数
- D. 他のユーザーからの参考情報

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

契約書には、一度にサイトを利用できる加入者数を明記する必要があります。

セキュリティ対策は契約の一部ではありませんが、重要な考慮事項です。

サードパーティサイトを選択する。購読者総数は考慮する必要はありません。重要なのは

契約が建物内または特定のエリア内の加入者数を制限しているかどうか。参照

他のユーザーが提供できるものは、契約締結前に考慮される事項であり、決して契約の一部ではありません。

契約条項。

最新問題: 326

Following the sale of a business division, employees will be transferred to a new organization, but they will retain access to IT equipment from the previous employer. An IS auditor has recommended that both organizations agree to and document an acceptable use policy for the equipment. What type of control has been recommended?

- A. Preventive control
- B. Directive control
- C. Corrective control
- D. Detective control

Answer: A ([メッセージを残す](#))

最新問題: 327

ソフトウェア開発においてプロトタイピング手法を用いる最大の利点は、以下の点に役立つことです。

- A. ユーザーテストとレビューに費やす時間を減らす
- B. システムの範囲変更を最小限に抑える
- C. 要件の概念化と明確化
- D. 品質保証 (QA) テストの効率を向上させる

Answer: (解答を表示する)

セクション：情報システムの取得、開発、導入

説明／参考資料：

最新問題: 328

Which of the following should be of GREATEST concern to an IS auditor reviewing the business continuity plan (BCP) of an organization with multiple vendors?

- A. Critical system interfaces are not documented or tested regularly.
- B. The recovery point objective (RPO) and recovery time objective (RTO) are the same.
- C. Recovery test plans are not updated annually.
- D. The business impact analysis (BIA) is only updated after a significant event.

Answer: A ([メッセージを残す](#))

最新問題: 329

ファイルサーバーに必要なデータ保護レベルを判断するための最適な情報源は次のうちどれですか？

- A. 過去のデータ漏洩事件報告
- B. 利用規約およびプライバシーに関する声明
- C. データ分類の方針と手順
- D. 類似ファイルサーバーのアクセス権限

Answer: C ([メッセージを残す](#))

最新問題: 330

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

- A. record the observations separately with the impact of each of them marked against each respective finding.
- B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
- C. record the observations and the risk arising from the collective weaknesses.
- D. apprise the departmental heads concerned with each observation and properly document it in the report.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined effect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

最新問題: 331

従業員のワークステーションにおけるソフトウェアライセンス違反に対処する最も効果的な方法はどれですか？

- A. 従業員のワークステーションにおける管理権限の制限
- B. ソフトウェアの自動インストールが必要
- C. 従業員のワークステーションにリアルタイム監視ソフトウェアを導入する
- D. ワークステーションを毎日スキャンして、不正なソフトウェアの使用がないか確認する

Answer: A ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 332

エンタープライズデータフローアーキテクチャにおいて、運用データ、外部データ、および非運用データからエンタープライズ情報を抽出するレイヤーは次のうちどれですか？

- A. データ準備層
- B. データソース層
- C. データマート層
- D. データアクセス層

Answer: B ([メッセージを残す](#))

セクション：情報システムの取得、開発、実装 説明：

企業情報は、以下の複数の情報源から得られます。

運用データ - 組織の既存システムによって取得および維持されるデータであり、通常はシステム固有のデータベースまたはフラットファイルに格納される。

外部データ - 外部の情報源から組織に提供されるデータ。これには、顧客の人口統計情報や市場シェア情報などが含まれる。

非運用データ - エンドユーザーが必要とする情報のうち、現在コンピュータでアクセス可能な形式で保存されていない情報。

CISA試験を受けるには、ビジネスインテリジェンスに関して以下の情報を知っておく必要があります。

ビジネスインテリジェンス (BI) は、意思決定を支援し、組織のパフォーマンスを評価するために情報を収集および分析する、ITの幅広い分野です。効果的なBIを実現するには、組織はデータアーキテクチャを設計および実装する必要があります。完全なデータアーキテクチャは、エンタープライズデータフローアーキテクチャ (EDFA) と論理データアーキテクチャの2つのコンポーネントで構成されます。このデータフローアーキテクチャのさまざまなレイヤー/コンポーネントは次のとおりです。

プレゼンテーション/デスクトップアクセス層 - エンドユーザーが情報に直接アクセスする層です。この層には、スプレッドシート、直接クエリツール、CongasやBusiness Objectsなどのベンダーが提供するレポート作成・分析スイートといった使い慣れたデスクトップツール、バランスソースカードやデジタルダッシュボードなどの専用アプリケーションが含まれます。

データソース層 - 企業情報は多数の情報源から得られる。

運用データ - 組織の既存システムによって取得および維持されるデータであり、通常はシステム固有のデータベースまたはフラットファイルに格納される。

外部データ - 外部の情報源から組織に提供されるデータ。これには、顧客の人口統計情報や市場シェア情報などが含まれる。

非運用データ - エンドユーザーが必要とする情報のうち、現在コンピュータでアクセス可能な形式で保存されていない情報。

コアデータウェアハウス - これは、組織にとって重要なすべてのデータが収集され、レポート作成や分析を支援するために整理される場所です。データウェアハウスは通常、大規模なリレーショナルデータベースとして構築されます。適切に構成されたデータウェアハウスは、3つの基本的な形式のクエリをサポートする必要があります。

ドリルアップとドリルダウン - ビジネスにとって重要なディメンションを使用することで、データの集計とドリルダウンが可能になります。データウェアハウスのより詳細なレベルで利用可能な属性を使用して、分析をさらに絞り込むこともできます。

ドリルスルー - 共通の属性を使用して、顧客別、および企業との取引期間に応じた顧客グループ別の全製品ラインの売上合計など、データウェアハウス内のさまざまな情報にアクセスします。

履歴分析 - 倉庫は、履歴データや時系列データを保持することで、この分析をサポートする必要があります。履歴分析の例としては、月ごとの店舗売上を報告し、年初に既に存在していた顧客のみを対象に分析を繰り返すことで、新規顧客の獲得効果と既存顧客からのリピート購入効果を区別することが挙げられます。

データマート層 - データマートは、コアデータウェアハウスから特定の事業部門または事業ラインのニーズを満たすように選択および整理された情報のサブセットを表します。データマートは、リレーショナルデータベースまたは何らかの形式のオンライン分析処理 (OLAP) データ構造である可能性があります。

データステージングおよび品質管理レイヤー - このレイヤーは、データのコピー、データウェアハウス (DW) 形式への変換、および品質管理を担当します。特に重要なのは、信頼性の高いデータのみがコアDWに格納されることです。このレイヤーは、アカウント番号形式の変更や古いアカウント番号および顧客番号の再利用など、運用システムによって定期的に発生する問題に対処できる必要があります。

データアクセス層 - この層は、データストレージ層とデータ品質層をデータソース層のデータストアに接続する役割を果たし、その過程で、これらのデータストアがどのように構成されているかを正確に知る必要性をなくします。現在の技術では、リレーショナルデータベースに格納されていないデータであっても、SQLを使用してデータにアクセスできます。

データ準備層 - この層は、データマートにロードするためのデータの組み立てと準備に関係します。アクセス速度を向上させるために、OLAPデータリポジトリにロードされる値を事前に計算するのが一般的な方法です。データマイニングは、大量のデータを探索して情報のパターンと傾向を特定することに関係します。データマイニングでは、データ関係の数と複雑さのために、直感に反するパターンが特定されることがよくあります。結果を損なわないように、データ品質は非常に高くなければなりません。

メタデータリポジトリ層 - メタデータとは、データに関するデータのことです。メタデータ層に保持される情報は、データ構造名やフォーマットにとどまらず、ビジネス上の目的やコンテキストに関する詳細情報を提供する必要があります。メタデータ層は包括的な範囲を持つべきであり、変換ルールや検証ルールの文書化を含め、さまざまな層間を流れるデータを網羅する必要があります。

ウェアハウス管理レイヤー - このレイヤーの機能は、データウェアハウスの構築と維持、およびデータマートへのデータ投入に必要なタスクのスケジュール設定です。このレイヤーはセキュリティ管理にも関与します。

アプリケーションメッセージング層 - この層は、さまざまな層間で情報を転送する役割を担います。ビジネスデータに加えて、この層は制御メッセージの生成、保存、および対象を絞った通信も行います。

インターネット／イントラネット層 - この層は基本的なデータ通信を扱います。ブラウザベースのユーザーインターフェースとTCP/IPネットワークが含まれます。

データアーキテクト／アナリストが使用するさまざまな分析モデルは以下のとおりです。

アクティビティ図またはスイムレーン図 - ビジネスプロセスを分解する。

エンティティ関係図 - データエンティティとその関係性を図示します。これらのデータ分析手法は、エンタープライズデータモデルの開発において重要な役割を果たします。しかし、知識豊富なビジネス担当者がプロセスに関与することも不可欠です。これにより、データのビジネス目的とコンテキストを適切に理解することができます。また、既存のシステムやデータベースから最適とは言えないデータ構成がデータウェアハウスに複製されるリスクも軽減されます。

以下の回答は誤りでした。

データマート層 - データマートは、コアデータウェアハウスから特定の事業部門または事業ラインのニーズを満たすように選択および整理された情報のサブセットを表します。データマートは、リレーショナルデータベースまたは何らかの形式のオンライン分析処理 (OLAP) データ構造である可能性があります。

データアクセス層 - この層は、データストレージ層とデータ品質層をデータソース層のデータストアに接続する役割を果たし、その過程で、これらのデータストアがどのように構成されているかを正確に知る必要性をなくします。現在の技術では、リレーショナルデータベースに格納されていないデータであっても、SQLを使用してデータにアクセスできます。

データ準備層 - この層は、データマートにロードするためのデータの組み立てと準備を担当します。アクセス速度を向上させるため、OLAPデータリポジトリにロードする値は事前に計算しておくのが一般的です。

参照：

CISAレビューマニュアル2014年版 188ページ

最新問題: 333

EDIアプリケーションで受信した注文の真正性を確保するための適切な管理策は次のとおりです。

- A. 電子注文の受領確認メッセージを送付する。
- B. 注文を処理する前に、注文数量の妥当性チェックを実施する。
- C. 送信者の身元を確認し、注文が契約条件に合致しているかどうかを判断します。
- D. 電子注文を暗号化する。

Answer: (解答を表示する)

説明／参考資料：

Explanation:

電子データ交換 (EDI) システムは、コンピュータシステムの一般的なリスクだけでなく、取引相手や第三者サービスプロバイダー側の管理体制の不備に起因するリスクにもさらされるため、ユーザーとメッセージの認証は重大なセキュリティ上の懸念事項となります。電子注文の受領確認メッセージで受領を通知することは適切な慣行ですが、顧客からの注文を認証するものではありません。注文前に注文数量の妥当性チェックを行うことは、自社の注文の正確性を確保するための管理策であり、顧客の注文の真正性を保証するものではありません。機密性の高いメッセージを暗号化することは適切な措置ですが、受信したメッセージには適用されません。

最新問題: 334

サイバー攻撃を受けた組織が、影響を受けたユーザーのコンピュータのフォレンジック分析を実施しています。このプロセスをレビューする情報システム監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？

- A. 各コンピュータからデータのコピーを取得するために、イメージング処理が使用されました。
- B. 法務部は関与していません。
- C. 保管管理の記録がありません。
- D. 監査は情報抽出時のみに関与した

Answer: (解答を表示する)

説明

証拠の保管管理記録が文書化されていないことは、サイバー攻撃を受けた組織のフォレンジック分析プロセスをレビューするIS監査担当者にとって、最も懸念すべき所見です。保管管理記録とは、フォレンジック調査中に証拠を取り扱った者、アクセスした者、または変更した者の記録です。保管管理記録を文書化することは、法廷における証拠の完全性、真正性、および許容性を維持するために不可欠です。その他の所見は、フォレンジック分析プロセスの妥当性や信頼性に影響を与えない可能性があり、それほど懸念すべき所見ではありません。参考文献：

CISAレビューマニュアル (デジタル版)、第7章、7.51節

最新問題: 335

An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

- A. Establish security metrics.
- B. Perform a penetration test
- C. Perform a configuration review
- D. Improve the change management process

Answer: C ([メッセージを残す](#))

最新問題: 336

An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

- A. There are conflicting permit and deny rules for the IT group
- B. There is only one rule per group with access privileges.
- C. Individual permissions are overriding group permissions.
- D. The network security group can change network address translation (NAT).

Answer: ([解答を表示する](#)**)**

最新問題: 337

ITプロジェクトおよびイニシアチブの優先順位付けにおける主要な基準として、以下のうちどれを使用すべきでしょうか？

- A. 概算費用と所要時間
- B. 期待される事業価値
- C. リスク低減レベル
- D. 利用可能なリソース

Answer: B ([メッセージを残す](#))

ITプロジェクトは、組織の戦略目標と整合し、ビジネス成果の面で最も大きな影響を与えるものでなければなりません。期待されるビジネス価値とは、収益の増加、コスト削減、効率性の向上、競争優位性など、プロジェクトが組織にもたらすメリットを指します。ビジネス価値に基づいてプロジェクトの優先順位付けを行うことで、投資対効果（ROI）や戦略的メリットが最も高い取り組みにリソースを確実に配分することができます。

コスト、時間、リスク軽減、利用可能なリソースといった要素は重要な考慮事項ではあるが、最も重要なのは、プロジェクトが組織全体の目標にどのように貢献し、ビジネス価値を生み出すかという点に焦点を当てることである。

最新問題: 338

IS監査人が各監査業務において考慮しなければならない最も重要なリスクは次のうちどれですか？

- A. プロセスとリソースの非効率性
- B. 不正行為および違法行為
- C. 組織の方針への不遵守
- D. 事業目標との不一致

Answer: D ([メッセージを残す](#))

IS監査人が各監査業務において考慮すべき最も重要なリスクは、事業目標との不整合です。これは、IS監査業務が、ITシステムとプロセスが事業目標と戦略の達成を支援していることを保証することを目的としているためです。不整合が生じると、リソースの浪費、機会損失、非効率性、エラー、または組織の業績と評判に悪影響を与える可能性のある障害が発生する可能性があります

12. 参考文献 :1 :CISAレビューマニュアル (デジタル版)、第1章：情報システム監査のプロセス、セクション1.3：監査リスク、ページ

28 2: CISAオンラインレビューコース、モジュール1: 情報システムの監査プロセス、レッスン1.3: 監査リスク

最新問題: 339

ビジネスプロセスオーナー向けのセキュリティトレーニングプログラムに、主に含めるべき項目は次のうちどれですか？

- A. アプリケーションの脆弱性
- B. 報告されたセキュリティインシデントの一覧
- C. アプリケーションの復旧時間
- D. セキュリティリスクの影響

Answer: D ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 340

When developing a business continuity plan (BCP), which of the following should be performed FIRST?

- A. Classify operations.
- B. Establish a disaster recovery plan (DRP)
- C. Conduct a business impact analysis (BIA)
- D. Develop business continuity training.

Answer: C ([メッセージを残す](#))

最新問題: 341

Which of the following BEST enables the effectiveness of an agile project for the rapid development of a new software application?

- A. Project milestones are created.
- B. The work is separated into phases.
- C. The work is separated into sprints.
- D. Project segments are established.

Answer: A ([メッセージを残す](#))

最新問題: 342

新しい電子商取引システムのデータベース制御をレビューしていた情報システム監査担当者が、データベース構成にセキュリティ上の脆弱性を発見しました。情報システム監査担当者が次に取り組むべき行動は次のうちどれでしょうか？

- A. 弱点を突く
- B. 既存の緩和策を特定する
- C. 調査結果を上級管理職に報告する

D. 是正措置の草案作成を支援する

Answer: ([解答を表示する](#))

最新問題: 343

以下の災害復旧／事業継続計画の構成要素のうち、災害後の復旧を最も確実に保証するものはどれですか？

- A.** 代替施設は、元の情報処理施設が復旧するまで利用可能です。
- B.** ユーザー管理は、重要なシステムとその関連する重要な復旧時間の特定に関与します。
- C.** 計画書のコピーは、主要な意思決定者の自宅に保管されている。
- D.** 経営陣に対し、事業継続計画が実際に実行可能であり、手順が最新であることを保証するフィードバックが提供されます。

Answer: A ([メッセージを残す](#))

災害後の復旧を最大限に確実にするためには、元の施設が復旧するまで代替施設を利用できるようにしておくべきである。この保証がなければ、計画は成功しない。その他の選択肢はすべて、計画の優先順位付けまたは実行を保証するものである。

最新問題: 344

Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

- A.** Systems logs
- B.** Access control lists (ACL)
- C.** Application logs
- D.** Error logs

Answer: B ([メッセージを残す](#))

Explanation/Reference:

IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

最新問題: 345

Security administration procedures require read-only access to:

- A.** access control tables.
- B.** security log files.
- C.** logging options.
- D.** user profiles.

Answer: B ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and user activities are monitored, captured, stored, processed and reported.

最新問題: 346

In order for a firewall to effectively protect a network against external attacks, what fundamental practice must be followed?

- A.** The firewall must be placed in the demilitarized zone (DMZ).
- B.** All external communication must be via the firewall.
- C.** Filters for external information must be defined.
- D.** Only essential external services should be permitted.

Answer: D ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 347

Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?

- A.** Parallel testing
- B.** Pilot testing
- C.** Interface/integration testing
- D.** Sociability testing

Answer: ([解答を表示する](#)**)**

Explanation/Reference:

Explanation:

The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system-and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure.

最新問題: 348

An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

- A.** cold site.
- B.** warm site.
- C.** dial-up site.

D. duplicate processing facility.

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

最新問題: 349

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

A. Blowfish

B. Tripwire

C. certificate

D. DES

E. one-time pad

F. None of the choices.

Answer: E ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

It's possible to protect messages in transit by means of cryptography. One method of encryption - the one- time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

最新問題: 350

When physical destruction is not practical, which of the following is the MOST effective measure of disposing of sensitive data on a hard disk?

A. Recycling the disk

B. Deleting files sequentially

C. Reformatting

D. Overwriting multiple times

Answer: A ([メッセージを残す](#))

最新問題: 351

データ分類ポリシーにおいて、定義することが最も重要なプロセスは次のうちどれですか？

A. データ資産の復旧

B. データ資産の処分

C. データ資産のバックアップ

D. データ資産へのアクセス監査

Answer: B ([メッセージを残す](#))

最新問題: 352

成熟した品質管理システム (QMS) を示す最良の指標は次のうちどれですか？

- A. 業界横断的なベンチマークが活用されています。
- B. 関連プロセスは継続的な改善を示している
- C. 関連するプロセスには文書化された品質目標があります
- D. 事業部門は最高品質責任者への報告ラインを持っています。

Answer: B ([メッセージを残す](#))

最新問題: 353

To reduce operational costs, IT management plans to reduce the number of servers currently used to run business applications. Which of the following is MOST helpful to review when identifying which servers are no longer required?

- A. Performance feedback from the user community
- B. Contract with the server vendor
- C. Server CPU usage trends
- D. Mean time between failure (MTBF) of each server

Answer: C ([メッセージを残す](#))

When identifying which servers are no longer required, reviewing server CPU usage trends is the most helpful approach.

Monitoring the CPU usage over time provides insights into how actively a server is being utilized.

Servers with consistently low CPU usage may be candidates for consolidation or decommissioning. By analyzing CPU utilization patterns, IT management can make informed decisions about which servers can be retired without impacting performance or availability¹.

References:

1.

ISACA. "Technical Guide on IT Migration Audit." 1(<http://kb.icai.org/pdfs/PDFFile5b278a12a66758.27269499.pdf>)

2. Zapier. "IT audit: The ultimate guide [with checklist]." 2(<https://zapier.com/blog/it-audit/>)

3. ISACA. "CISA Certification | Certified Information Systems Auditor." 3(<https://www.isaca.org/credentialing/cisa>)

最新問題: 354

IS監査担当者がフォローアップの内部IS監査を実施し、いくつかの推奨事項が

前年度の施策が実施されていない場合、監査人が最初に行うべきことは次のうちどれでしょうか。アクション？

- A. 現在のIT環境を踏まえて推奨事項を評価する。
- B. 監査を継続し、以前の監査勧告を無視する。
- C. 前年度からの提言を経営陣に実施するよう要請する。
- D. 未実施の推奨事項を新たな監査の所見として追加する。

Answer: D ([メッセージを残す](#))

セクション: 情報資産の保護

最新問題: 355

Which of the following would BEST assist senior management in evaluating IT performance as well as the alignment between corporate and IT strategic objectives?

- A. IT project value analysis
- B. Control self-assessment
- C. Balanced scorecard
- D. Enterprise architecture

Answer: C ([メッセージを残す](#))

最新問題: 356

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- A. Optimized
- B. Managed
- C. Defined
- D. Repeatable

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

最新問題: 357

組織の業務上重要なサーバーハードウェアのオンサイト予防保守をレビューするIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？

- A. 予防保全スケジュールは、平均故障間隔 (MTBF) パラメータに基づいています。
- B. 予防保全費用が事業予算を超えている。
- C. 予防保守は情報システム所有者によって承認されていません。
- D. 予防保守は、秘密保持契約 (NDA) を必要とせずに複数のベンダーにアウトソーシングされます。

Answer: C ([メッセージを残す](#))

最新問題: 358

Which of the following is the MOST important responsibility of user departments associated with program changes?

- A. Updating documentation to reflect latest changes
- B. Providing unit test data
- C. Analyzing change requests
- D. Approving changes before implementation

Answer: B ([メッセージを残す](#))

最新問題: 359

仮想環境でゲストオペレーティングシステムを利用する最大の利点は次のうちどれですか？

- A. 環境への影響を最小限に抑えつつ、容器への詰め込みが容易です。
- B. どの場所からでもログインして監視できます。
- C. セキュリティ侵害が発生した場合、迅速に消去できます。
- D. 伝送制御プロトコル/インターネットプロトコル (TCP/IP) を介して、より広い環境へのアクセスを阻止します。

Answer: C ([メッセージを残す](#))

最新問題: 360

内部監査では、顧客取引リスクの監査を実施しています。データ分析を使用する最適な理由は次のうちどれでしょうか？

- A. データセット内の異常値とリスク傾向はまだ定義されていません
- B. トランザクションデータは、信頼性のレベルが異なる複数の独立したシステムに格納されています。
- C. この監査は、定期的な無作為抽出検査を義務付ける規制を遵守するために実施されています。
- D. 監査の焦点は、事前に定義された少数の高リスク取引に絞られています。

Answer: B ([メッセージを残す](#))

最新問題: 361

In which of the following database model is the data organized into a tree-like structure, implying a single parent for each record?

- A. Hierarchical database model
- B. Network database model
- C. Relational database model
- D. Object-relational database model

Answer: A ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

Explanation/Reference:

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record.

A sort field keeps sibling records in a particular order.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

Hierarchical database model

Network model

Relational model

Object-relational database models

Hierarchical database model

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information. This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model



Network database model

The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of

B. At the

same time another set may be defined where B is the owner of

A. Thus all the sets comprise a general

directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model,

and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.

Network Database model



Relational database model

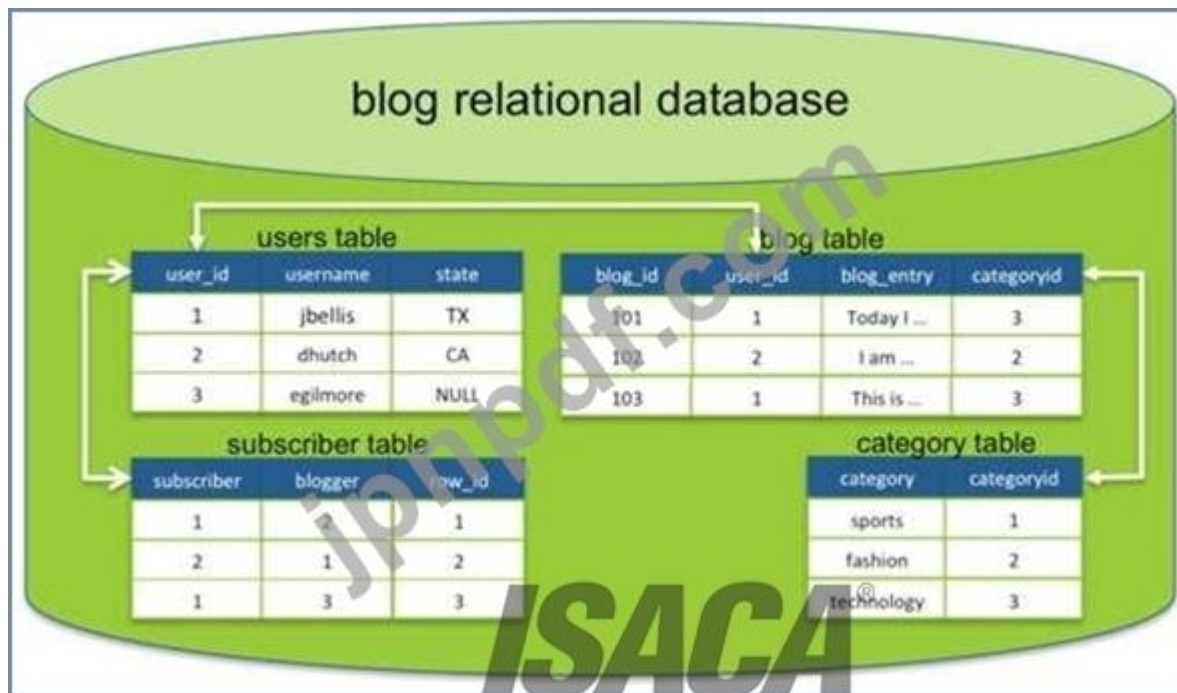
In the relational model of a database, all data is represented in terms of tuples, grouped into relations. A database organized in terms of the relational model is a relational database.

In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.

Relational database model



Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Network model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

Relational model- In the relational model of a database, all data is represented in terms of tuples, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following reference(s) were/was used to create this question:

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 362

セキュリティ設定を積極的に強化するために、最も関連性の高い情報を提供するのはいずれですか？

- A. バスティアオンホスト
- B. 侵入検知システム
- C. ハニーポット
- D. 侵入防止システム

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

ハニーポットは、ハッカーをおびき寄せ、ハッカーの手法や戦略、そして攻撃に対処するために必要なリソースに関する手がかりを提供するように設計されています。一方、バスティアオンホストは攻撃に関する情報を提供しません。侵入検知システム (IDS) と侵入防御システム (IPS) は、進行中の攻撃を検知して対処し、できるだけ早く攻撃を阻止するように設計されています。ハニーポットは、ハッカーの戦略や手法に関する情報を得るために、攻撃を継続させます。

最新問題: 363

The PRIMARY benefit of information asset classification is that it:

- A. prevents loss of assets.
- B. helps to align organizational objectives.
- C. facilitates budgeting accuracy.
- D. enables risk management decisions.

Answer: D ([メッセージを残す](#))

Explanation

The primary benefit of information asset classification is that it enables risk management decisions.

Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 300

最新問題: 364

IS監査担当者が、運用サポートチームのインシデント管理手順をレビューし、適切な優先順位付け基準が定義されているかどうかを評価しています。優先順位付け基準に含めるべき最も重要な項目は次のうちどれですか？

- A. ビジネスへの影響
- B. 復元ポイント
- C. 修復費用
- D. 修理の時間

Answer: A ([メッセージを残す](#))

最新問題: 365

IT部門は、ベンダーから提供された重要なパッチを人事部の運用サーバーにインストールしました。インストール完了直後、人事部から、どのユーザーもシステムにアクセスできないとの報告がありました。この問題に対処するために、IT部門が最初にとるべき手順は何でしょうか？

- A. ステージングサーバーでシステム診断を実行します。
- B. 通話内容とユーザーの問題を文書化する。
- C. システムのトラブルシューティングを行い、問題を修正します。
- D. バックアウト手順に従ってください

Answer: D ([メッセージを残す](#))

最新問題: 366

Who is accountable for maintaining appropriate security measures over information assets?

- A. Data and systems owners
- B. Data and systems users
- C. Data and systems custodians
- D. Data and systems auditors

Answer: ([解答を表示する](#))

Explanation/Reference:

Data and systems owners are accountable for maintaining appropriate security measures over information assets.

最新問題: 367

In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

- A. application programmer copy the source program and compiled object module to the production libraries
- B. application programmer copy the source program to the production libraries and then have the production control group compile the program.
- C. production control group compile the object module to the production libraries using the source program in the test environment.
- D. production control group copy the source program to the production libraries and then compile the program.

Answer: D ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

最新問題: 368

Which of the following will enable a customer to authenticate an online Internet vendor?

- A. Vendor signs a reply using a hash function and the customer's public key.
- B. Customer verifies the vendor's certificate with a certificate authority (CA).
- C. Vendor decrypts incoming orders using its own private key.
- D. Customer encrypts an order using the vendor's public key.

Answer: B ([メッセージを残す](#))

最新問題: 369

A global company has been using a publicly available AI tool to obtain information about global laws and regulations that could impact the business. Which of the following should be of MOST concern to an IS auditor?

- A. Accuracy and quality of the data provided by the AI tool
- B. Whether the organization is using a paid version of the AI tool
- C. Version and provider of the AI tool being utilized
- D. Whether the tool is utilized by competitors in the same industry

Answer: A ([メッセージを残す](#))

最大のリスクは、不正確または質の低い法律 規制情報に依存してしまうことであり、これは法令遵守違反につながる可能性があります。その他の懸念事項（有料プラン、プロバイダー、競合他社など）は二次的なものです。

最新問題: 370

A database is denormalized in order to:

- A. increase processing efficiency.
- B. ensure data integrity.
- C. save storage space.
- D. prevent loss of data.

Answer: A ([メッセージを残す](#))

最新問題: 371

システム保守プログラムの有効性を判断する際に、情報システム監査担当者にとって非常に役立つものは何でしょうか？最も適切な回答を選択してください。

- A. ネットワーク監視ソフトウェア
- B. システムダウンタイムログ
- C. 管理活動報告
- D. ヘルプデスク利用動向レポート

Answer: (解答を表示する)

説明／参考資料：

システム停止ログは、情報システム監査担当者がシステム保守プログラムの有効性を判断する際に非常に役立ちます。

最新問題: 372

以下のリスクシナリオのうち、フルディスク暗号化に関連するポリシーと手順を導入することで最も効果的に対処できるのはどれですか？

- A. 従業員が競合他社に転職したことによるデータ漏洩
- B. 規制対象情報の保管に関する法令違反に対する罰金
- C. アプリケーションインターフェースを介した情報への不正な論理アクセス
- D. 情報が保存されている媒体の物理的な盗難

Answer: D ([メッセージを残す](#))

説明

フルディスク暗号化 (FDE) は、一時ファイル、プログラム、システムファイルを含むディスク上のすべてのデータを暗号化することで情報を保護する手段です¹。FDEは、情報が保存されているメディアの物理的な盗難というリスクシナリオに対処するのに最適です。デバイスが紛失または盗難された場合でも、データへの不正アクセスを防ぐことができます²。FDEは、従業員が競合他社に転職した場合のデータ漏洩を防ぐことはできません。従業員は、デバイスを使用している間、または退職前にデータを別のデバイスにコピーしている間、データにアクセスできる可能性があるためです。FDEは、規制対象情報の保存に関連する法令違反の罰金を防ぐことはできません。データが適用される法律および規制に従って保存されることを保証するものではないためです。FDEは、ユーザーおよびアプリケーションのアクセス権限とアクセス許可を制御しないため、アプリケーションインターフェースを介した情報への不正な論理アクセスを防ぐことはできません。^{*}参照 : ISACA IT監査および保証基準、IS監査および保証専門家のためのガイドラインおよびツールとテクニック、セクション

2402 計画、IS 監査および保証の専門家は、レビュー対象領域に関連するリスクを特定し、評価する必要があります。」³ 考慮すべきリスク要因の 1 つは、システムによって処理、保存、または送信される情報の機密性」³ です。FDE は、メディアの物理的な盗難による機密情報の不正な開示のリスクを軽減するための可能な制御の 1 つです。

最新問題: 373

Which of the following is the GREATEST concern with conducting penetration testing on an internally developed application in the production environment?

- A. The testing could create application availability issues.
- B. The testing may identify only known operating system vulnerabilities.
- C. テスト中に特定された問題には、相当な修復作業が必要となる可能性があります。
- D. 内部セキュリティ担当者は、アプリケーションの侵入テストを実施する資格がない可能性があります。

Answer: D ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

説明／参考資料：

最新問題: 374

IS監査人が新しい機器の取得をレビューする場合、次のうちどれが重大な弱点？

- A. 評価に関わったスタッフは、評価対象のベンダーを認識していました。
- B. 独立コンサルタントが提案依頼書 (RFP) 文書を作成した。
- C. 評価基準は、回答の初期評価後に最終決定されました。

D. 潜在的なベンダーからの要請を受けて、回答の締め切り日が延長されました。

Answer: C ([メッセージを残す](#))

セクション：情報システムの取得、開発、導入

最新問題: 375

Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?

A. Water sprinkler

B. Fire extinguishers

C. Carbon dioxide (CO2)

D. Dry pipe

Answer: C ([メッセージを残す](#))

Explanation

無人コンピュータ室における最も適切かつ効果的な消火方法は、二酸化炭素 (CO2) です。二酸化炭素は、酸素を置換して燃焼プロセスを抑制することで消火する気体状のクリーン消火剤です。二酸化炭素は、電子機器に残留物、損傷、腐食を残さず、環境や人体に害を及ぼす可能性のある水やその他の化学物質を必要としないため、無人コンピュータ室に適しています。ただし、二酸化炭素は、放出中または放出後にコンピュータ室に入った人に窒息の危険性があるため、適切な安全対策と警告標識を設置する必要があります。

無人コンピュータ室においては、二酸化炭素ほど適切かつ効果的な選択肢は他にない。

散水式消火器。これは、水を使って火災を冷却・消火する一般的な消火方法です。しかし、散水式消火器は、ショート、腐食、データ損失など、電子機器に深刻な損傷を与える可能性があるため、無人のコンピュータ室には適していません。また、散水中または散水後にコンピュータ室に入った人が感電する危険性もあります。

消火器。これらは、加圧された消火剤を噴射して火を消す携帯型の装置です。しかし、消火器は、火災の種類と場所を特定し、適切な消火器を使用できる訓練を受けた人による手動操作が必要なため、無人のコンピュータ室では効果的ではありません。また、消火器に水や化学薬品が含まれている場合、電子機器に損傷を与える可能性があります。

ドライパイプ式スプリンクラーは、火災が検知されるまで配管内に水ではなく加圧空気または窒素を使用するタイプのスプリンクラーシステムです。火災が検知されると、空気または窒素が放出され、水が配管とスプリンクラーに流れ込みます。ただし、ドライパイプ式は消火剤として水を使用するため、前述のように電子機器を損傷する可能性があり、無人コンピュータ室には適していません。

乾式配管は湿式配管スプリンクラーシステムよりも反応時間が遅いため、火災がより速く広がる可能性がある。

最新問題: 376

Which of the following is MOST important to define within a disaster recovery plan (DRP)?

A. Test results for backup data restoration

B. A comprehensive list of disaster recovery scenarios and priorities

C. Business continuity plan (BCP)

D. Roles and responsibilities for recovery team members

Answer: B ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 377

次のうち、データ検証の編集と制御に該当するものはどれですか？

- A. ハッシュ合計
- B. 妥当性チェック
- C. オンラインアクセス制御
- D. ビフォーアフター画像レポート

Answer: (解答を表示する)

説明／参考資料：

Explanation:

妥当性チェックとは、データが事前に定められた基準に準拠していることを確認するために使用される、データ検証のための編集および管理のことです。

不正解：

- A. ハッシュ合計とは、データファイル内の任意の数値データフィールドまたは一連のデータ要素の合計です。この合計は、同じフィールドまたは複数のフィールドの制御合計と比較され、処理の完全性が確認されます。
- B. オンラインアクセス制御は、システムおよびデータへの不正アクセスを防止するように設計されています。
- C. 前後画像レポートは、変更を追跡できるようにするデータファイルの制御です。

最新問題: 378

An IS auditor is reviewing the results of a business process improvement project. Which of the following should be performed FIRST?

- A. Evaluate control gaps between the old and the new processes.
- B. Develop compensating controls.
- C. Document the impact of control weaknesses in the process.
- D. Ensure that lessons learned during the change process are documented.

Answer: A (メッセージを残す)

Section: Protection of Information Assets

最新問題: 379

An organization's enterprise architecture (EA) department decides to change a legacy system's components while maintaining its original functionality. Which of the following is MOST important for an IS auditor to understand when reviewing this decision?

- A. The current business capabilities delivered by the legacy system
- B. The proposed network topology to be used by the redesigned system
- C. The data flows between the components to be used by the redesigned system
- D. The database entity relationships within the legacy system

Answer: ([解答を表示する](#))

Explanation

When reviewing an enterprise architecture (EA) department's decision to change a legacy system's components while maintaining its original functionality, an IS auditor should understand the current business capabilities delivered by the legacy system, as this would help to evaluate whether the change is justified, feasible, and aligned with the business goals and needs. The proposed network topology to be used by the redesigned system, the data flows between the components to be used by the redesigned system, and the database entity relationships within the legacy system are technical details that are less relevant for an IS auditor to understand when reviewing this decision. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

最新問題: **380**

監査の際、データ品質を測定するための基準値を設定する上で、次のうちどれが最も役立ちますか？

- A. お客様からのご意見
- B. 内蔵データエラー防止アプリケーション制御
- C. 業界標準のビジネス定義
- D. ビジネスによるルールの検証

Answer: D ([メッセージを残す](#))

最新問題: **381**

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- A. Enforce an internal data access policy.
- B. Apply single sign-on for access control
- C. Enforce the use of digital signatures.
- D. Implement segregation of duties.

Answer: A ([メッセージを残す](#))

最新問題: **382**

時間制約のあるシステムやトランザクションに対して、ほぼ即時の復旧性を提供するものはどれですか？
処理？

- A. 自動電子ジャーナリングと並列処理
- B. データミラーリングと並列処理
- C. データミラーリング
- D. 並列処理

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

データミラーリングと並列処理はどちらも、ほぼ即座にデータを復元できるようにするために使用され、機密性の高いシステムおよびトランザクション処理。

最新問題: 383

Which of the following is the BEST indication of effective governance over IT infrastructure?

- A. An increase in the number of IT infrastructure servers
- B. A requirement for annual security awareness programs
- C. A decrease in the number of information security incidents
- D. The ability to deliver continuous, reliable performance

Answer: D ([メッセージを残す](#))

最新問題: 384

次の攻撃のうち、偽造された ICMP エコー要求パケットをブロードキャストに送信するものはどれですか。
複数のゲートウェイにアドレスを設定し、ゲートウェイの背後にあるコンピュータから不正な応答を引き出す。
それらはすべて、ICMPエコー要求の送信元IPアドレスにICMPエコー応答パケットで応答します。
パケット？

- A. 反射攻撃
- B. 力任せの攻撃
- C. バッファオーバーフロー
- D. 脈動するゾンビ

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

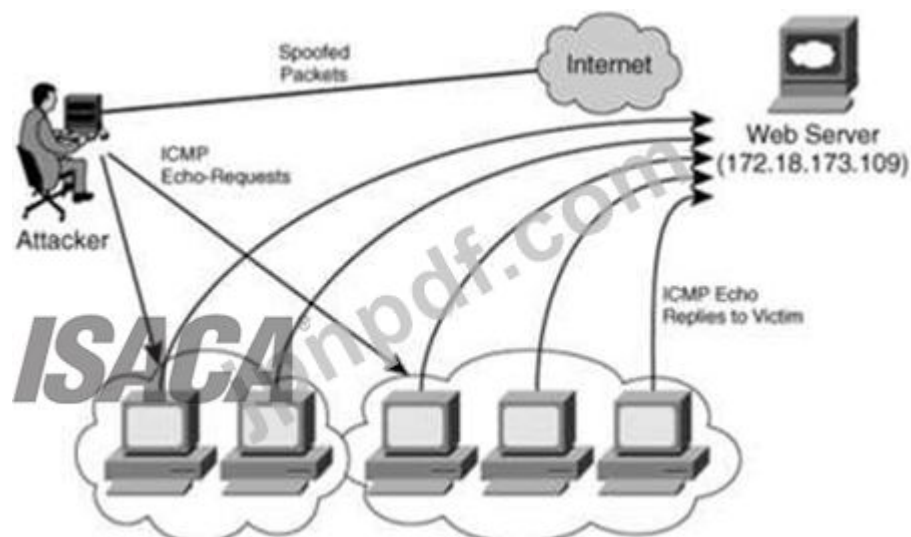
説明／参考資料：

反射攻撃とは、多数のコンピュータに偽造されたリクエストを送信し、それらのコンピュータがリクエスト。送信元IPアドレスは標的の被害者のIPアドレスに偽装され、応答が大量に送信される。
分散型サービス拒否攻撃では、非常に大規模なネットワークに何らかの偽造リクエストを送信することが含まれる場合があります。
要求に応答するコンピュータの数。インターネットプロトコルアドレスの偽装を使用すると、送信元はアドレスは標的の被害者のアドレスに設定されているため、すべての応答は標的に送られ (そして標的に殺到する) こととなります。
(この反射型攻撃は「DRDOS」と呼ばれることもあります。)

ICMPエコー要求攻撃 (スマーフ攻撃)は、フラッディング攻撃の一種である反射攻撃とみなすことができる。
ホストは、混合構成ネットワークのブロードキャスト アドレスにエコー リクエストを送信し、ホストを誘引します。
被害者にエコー応答パケットを送信する。初期のDDoSプログラムの中には、分散型のこの攻撃。

サーフ攻撃では、攻撃者は偽装した送信元アドレスを持つICMP ECHO REQUESTパケットを送信します。
被害者のネットワークブロードキャストアドレス。これは、被害者のサブネット上の各システムが、ICMP ECHO REQUEST パケット。各システムは、その要求に対して ICMP ECHO REPLY パケットで応答します。
パケットは、パケットで指定された偽装アドレス (被害者のアドレス)に送信されます。これらの応答はすべてパケットは被害者システムに到達し、大量のパケットで攻撃されるため、システムを圧倒します。
必ずしも処理方法を知っている必要はありません。被害を受けたシステムはフリーズ、クラッシュ、または再起動する可能性があります。Smurf攻撃は
下図に示すように。

サーフアタック



以下の回答は誤りです。

ブルートフォース攻撃 - ブルートフォース (ブルートフォースクラッキングとも呼ばれる)は、試行錯誤の方法であり、パスワードやデータ暗号化標準 (DES)などの暗号化されたデータを復号化するアプリケーションプログラム

鍵は、知的な戦略を用いるのではなく、徹底的な努力 (ガク)によって入手する。

アプリケーションは、有効な文字の可能なすべての組み合わせを順番に処理します。総当たり攻撃は

時間がかかるものの、確実な方法と考えられている。

バッファオーバーフロー - プログラムまたはプロセスがバッファにこれ以上データを格納しようとしたときにバッファオーバーフローが発生します。

(一時データ記憶領域)は、本来保持するはずだった容量よりも多くなります。

データ量が増えると、余分な情報 (どこかに収めなければならない)が隣接するバッファに溢れ出す可能性があります。

それらに保持されている有効なデータを破損または上書きすること。

プログラミングエラーであるバッファオーバーフローは、データ整合性に対するセキュリティ攻撃としてますます一般的になっている。

パルシングゾンビ - 複数の攻撃者によるネットワークへの悪意のあるピング攻撃を行うDoS攻撃

長期間にわたるコンピュータの使用。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 322ページ

最新問題: 385

在庫アプリケーションの監査において、どの方法が購入の最良の証拠を提供するか
注文は有効ですか？

- A. 不適切な担当者がアプリケーションパラメータを変更できるかどうかをテストする
- B. 購入注文をコンピュータのリストに紐付ける
- C. 受領報告書と発注書の詳細を比較する
- D. 申請書類の確認

Answer: A ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

発注書の有効性を判断するには、アクセス制御をテストすることが最良の証拠となります。選択肢BとCは事後的なアプローチに基づいているが、選択肢Dは目的に合わない。
システムドキュメントの内容と実際の状況は一致しない場合があります。

最新問題: 386

継続的監査アプローチの利点は、多数のトランザクションを処理するタイムシェアリング環境で使用する場合に、システムセキュリティを向上させることができる点である。正誤を答えよ。

A. 真の

B. 偽

Answer: ([解答を表示する](#))

セクション: 情報資産の保護

Explanation:

確かに、継続的な監査アプローチの利点の一つは、多数のトランザクションを処理するタイムシェアリング環境で使用する場合に、システムセキュリティを向上させることができる点である。

最新問題: 387

Which of the following should be the PRIMARY role of an internal audit function in the management of identified business risks?

A. Validating enterprise risk management (ERM)

B. Operating the risk management framework

C. Establishing a risk management framework

D. Establishing a risk appetite

Answer: ([解答を表示する](#))

最新問題: 388

Which of the following is the PRIMARY benefit of implementing an IT capacity management process?

A. Ensuring infrastructure meets current performance requirements

B. Enabling rapid deployment of new software applications

C. Helping resolve significant security concerns

D. Reducing the cost and time to implement IT services

Answer: A ([メッセージを残す](#))

Comprehensive and Detailed Explanation:

The primary purpose of IT capacity management is to ensure that IT infrastructure can meet current and future performance requirements in a cost-effective manner.

Option A is correct because it directly relates to capacity management goals.

Option B (rapid deployment) relates more to change management.

Option C (security concerns) is outside the scope of capacity management.

Option D (reducing cost/time) may be a secondary benefit but not the primary objective.

ISACA Reference: CISA Review Manual 27th Edition, Domain 2, section on capacity management and IT service performance.

最新問題: 389

経営陣に対し、ITに関する内部統制について利害関係者への報告書の発行を義務付けることの利点として、次のうちどれが挙げられますか？

- A. ITコストの透明性
- B. ポートフォリオ管理の改善
- C. コスト管理の改善
- D. ITガバナンスに注力

Answer: D ([メッセージを残す](#))

セクション :ITのガバナンスと管理

最新問題: 390

In a public key cryptographic system, which of the following is the PRIMARY requirement to address the risk of man-in-the-middle attacks through spoofing?

- A. Strong encryption algorithms
- B. Kerberos authentication
- C. Registration authority
- D. Certificate authority (CA)

Answer: D ([メッセージを残す](#))

A certificate authority (CA) is critical in a public key cryptographic system for mitigating man-in-the-middle (MITM) attacks. It ensures that public keys are authentic by issuing digital certificates, which bind a public key to an entity. The CA's role in verifying identities and providing trust anchors prevents attackers from spoofing keys.

* Strong Encryption Algorithms (Option A):Encryption ensures confidentiality but does not address spoofing risks.

* Kerberos Authentication (Option B):Useful for mutual authentication but not central to public key infrastructure (PKI).

* Registration Authority (Option C):Supports the CA but does not directly prevent MITM attacks.

Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

最新問題: 391

システムリソースの命名規則は、アクセス制御において重要です。なぜなら、次のような理由があるからです。

- A. リソース名があいまいでないことを確認してください。
- B. 資源を適切に保護するために必要な規則の数を減らす。
- C. リソースへのユーザーアクセスが明確かつ一意に識別されるようにします。
- D. 国際的に認知された名称を使用して資源を保護する。

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

システムリソースの命名規則は、セキュリティ制御を効率的に管理するために重要です。

The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous

cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 392

When reviewing past results of a recurring annual audit, an IS auditor notes that findings may not have been reported and independence may not have been maintained Which of the following is the auditor's BEST course of action?

- A. Inform audit management
- B. Inform senior management
- C. Reevaluate internal controls
- D. Re-perform past audits to ensure independence

Answer: A ([メッセージを残す](#))

最新問題: 393

すべてのシステムのバックアップに関する考慮事項に加えて、オンラインシステムのバックアップを提供する上で重要な考慮事項は次のうちどれですか？

- A. システムソフトウェアパラメータの維持
- B. トランザクションログの定期的なダンプを確保する
- C. 祖父・父・息子のファイルバックアップを確実に行う
- D. 重要なデータをオフサイトの場所に保管する

Answer: B ([メッセージを残す](#))

トランザクションログを定期的にダンプすることが、タイムリーな履歴データを確実に保存する唯一の方法です。オンラインシステムでは通常、大量のアクティビティが発生するため、他の従来型のバックアップ方法は実用的ではありません。

最新問題: 394

IS監査チームが、最新のアプリケーションユーザーアクセスレビューに関する文書を評価している。

ユーザーリストがシステムによって生成されたものではないことが判明しました。以下のうち、最も懸念すべき点はどれでしょうか？

- A. ユーザーリストの入手可能性
- B. ユーザーリストの機密保持
- C. ユーザーリストの完全性
- D. ユーザーリストレビューの適時性

Answer: C ([メッセージを残す](#))

最新問題: 395

職務分掌を適切に行うことで、コンピュータオペレーター（ユーザー）がセキュリティ管理業務を行うことを防ぐことができる。
正誤を答えよ。

- A. 真
- B. 偽

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

適切な職務分掌により、コンピュータオペレーター（ユーザー）がセキュリティ管理業務を行うことを防ぐことができる。

最新問題: 396

Intrusion detection systems (IDSs) can:

- A. compensate for weak authentication mechanisms
- B. conduct investigations of attacks from within the network
- C. provide information to enhance the security infrastructure.
- D. substitute for a firewall.

Answer: C ([メッセージを残す](#))

最新問題: 397

Which of the following correctly describes the purpose of an Electronic data processing audit?

- A. to collect and evaluate evidence of an organization's information systems, practices, and operations.
- B. to ensure document validity.
- C. to verify data accuracy.
- D. to collect and evaluate benefits brought by an organization's information systems to its bottomline.
- E. None of the choices.

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

An Electronic data processing (EDP) audit is an IT audit. It is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations.

最新問題: 398

ダイヤルアップ高速応答システムに保存されているデータへの不正アクセスを防止するために、IS監査担当者は推奨すべき事項：

- A. オンライン端末は制限区域に設置されています。
- B. オンライン端末には鍵付きロックが装備されています。
- C. オンライン端末へのアクセスにはIDカードが必要です。
- D. 指定された回数の試行失敗後、オンラインアクセスは終了します。

Answer: D ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

不正アクセスを防止するための最も適切な制御方法は、指定された時間後に接続を終了することです。
試行回数。これにより、IDやパスワードの推測によるアクセスを阻止できます。その他の選択肢
これらは物理的な対策であり、電話回線を介した不正アクセスを阻止するには効果的ではない。

最新問題: 399

Which of the following type of network service stores information about the various resources in a central database on a network and help network devices locate services?

- A. DHCP
- B. DNS
- C. Directory Service
- D. Network Management

Answer: C ([メッセージを残す](#))

Explanation/Reference:

A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.

Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:

Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.

Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information.

Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.

Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

最新問題: 400

IS監査担当者は、経営陣の回答に対してまず何をすべきでしょうか？

対面式の内部統制質問票は、重要な内部統制を示す。

制御はもはや効果的ではないのか？

A. 制御を行うために必要なリソースを決定する

効果的。

B. 内部統制の全体的な有効性を検証する。

C. Verify the impact of the control no longer being effective.

D. Ascertain the existence of other compensating controls.

Answer: D (メッセージを残す)

The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness. The other options are not the first steps, because they either require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

最新問題: 401

Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

- A. Creating communication channels
- B. Promoting security training
- C. Establishing a steering committee
- D. Holding periodic meetings with business owners

Answer: B ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: 402

IS監査担当者が環境管理をレビューしたところ、データセンター内で極めて高い湿度レベルが発見されました。この状況によってコンピュータ機器に生じる主なリスクは次のうちどれですか？

- A. 静電気
- B. 火
- C. 腐食
- D. 停電

Answer: A ([メッセージを残す](#))

最新問題: 403

Which of the following is the key benefit of control self-assessment (CSA)?

- A. Management ownership of the internal controls supporting business objectives is reinforced.
- B. Audit expenses are reduced when the assessment results are an input to external audit work.
- C. Improved fraud detection since internal business staff are engaged in testing controls
- D. Internal auditors can shift to a consultative approach by using the results of the assessment.

Answer: (解答を表示する)

内部統制自己評価の目的は、経営陣が内部統制の重要性和コーポレートガバナンスにおける自らの責任をより深く認識することです。監査費用の削減は、内部統制自己評価 (CSA) の主要なメリットではありません。不正検出の改善は重要ですが、所有権ほど重要ではなく、CSAの主要な目的ではありません。CSAは内部監査人に多くの洞察を与え、よりコンサルティング的な役割を担うことを可能にするかもしれませんが、これは付加的なメリットであり、主要なメリットではありません。

トピック3 :ITガバナンス（練習問題11問）

最新問題: 404

正しいテキスト

人事担当副社長は、前年度の給与過払いを特定するための監査を依頼しました。この状況において、最も適切な監査手法はどれでしょうか？

- A) テストデータ
- B. 汎用監査ソフトウェア
- C. 総合試験施設
- D. 組み込み監査モジュール

Answer:

B

Explanation:

汎用監査ソフトウェアの機能には、数学的計算、層別化、統計分析、順序チェック、重複チェック、再計算などが含まれます。IS監査担当者は、汎用監査ソフトウェアを使用して、給与を再計算するための適切なテストを設計し、過払いがあったかどうか、また誰に過払いがあったかを判断できます。テストデータは、過払いを防止する可能性のある統制の存在をテストしますが、特定の過去の計算ミスを検出することはできません。統合テスト機能も組み込み監査モジュールも、過去の期間のエラーを検出することはできません。

最新問題: 405

Validated digital signatures in an e-mail software application will:

- A. help detect spam.
- B. provide confidentiality.
- C. add to the workload of gateway servers.
- D. significantly reduce available bandwidth.

Answer: ([解答を表示する](#))

Validated electronic signatures are based on qualified certificates that are created by a certification authority (CA), with the technical standards required to ensure the key can neither be forced nor reproduced in a reasonable time. Such certificates are only delivered through a registration authority (RA) after a proof of identity has been passed. Using strong signatures in e-mail traffic, nonrepudiation can be assured and a sender can be tracked. The recipient can configure their e-mail server or client to automatically delete e-mails from specific senders. For confidentiality issues, one must use encryption, not a signature, although both methods can be based on qualified certificates. Without any filters directly applied on mail gateway servers to block traffic without strong signatures, the workload will not increase. Using filters directly on a gateway server will result in an overhead less than antivirus software imposes. Digital signatures are only a few bytes in size and will not slash bandwidth. Even if gateway servers were to check CRLs, there is little overhead.

最新問題: 406

プロセス内の予防的、発見的、または是正的統制の総合的な効果を適切に評価するために、IS監査人は次のうちどれを認識しておくべきでしょうか？

- A. 組織の事業目標
- B. 職務分掌が内部統制に及ぼす影響
- C. システムがデータフローを流れる際に制御が行われるポイント
- D. 組織統制方針

Answer: ([解答を表示する](#))

セクション：情報資産の保護

説明

Explanation:

プロセス内の予防的、検出的、または是正的統制の総合的な効果を評価する際、IS監査人は、データがシステムを通過する際に統制が実行されるポイントを認識しておく必要がある。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 407

Which of the following should be the FIRST step when developing a data loss prevention (DLP) solution for a large organization?

- A. Identify approved data workflows across the enterprise.
- B. Conduct a threat analysis against sensitive data usage.
- C. Create the DLP policies and templates
- D. Conduct a data inventory and classification exercise

Answer: ([解答を表示する](#))

Explanation

The first step when developing a data loss prevention (DLP) solution for a large organization is to conduct a data inventory and classification exercise. This step is essential to identify the types, locations, owners, and sensitivity levels of the data that need to be protected by the DLP solution. A data inventory and classification exercise helps to define the scope, objectives, and requirements of the DLP solution, as well as to prioritize the data protection efforts based on the business value and risk of the data. A data inventory and classification exercise also enables the organization to comply with relevant laws and regulations regarding data privacy and security.

The other options are not the first step when developing a DLP solution, but rather subsequent steps that depend on the outcome of the data inventory and classification exercise. Identifying approved data workflows across the enterprise is a step that helps to design and implement the DLP policies and controls that match the business processes and data flows. Conducting a threat analysis against sensitive data usage is a step that helps to assess and mitigate the risks associated with data leakage, theft, or misuse. Creating the DLP policies and templates is a step that helps to enforce the data protection rules and standards across the organization.

References:

ISACA CISA Review Manual 27th Edition (2019), page 247

Data Loss Prevention-Next Steps - ISACA1

What is data loss prevention (DLP)? | Microsoft Security

最新問題: 408

2つのインターネット接続を持つ組織ネットワークの回復力を監査するIS監査担当者にとって、以下のうちどれが最も懸念されるでしょうか？

- A. 重要度の低いアプリケーションも両方の接続に接続されます。
- B. 両方の接続は同じプロバイダーからのものです。
- C. 事業継続計画 (BCP)は過去6か月間テストされていません。
- D. ネットワーク容量テストは実施されていません。

Answer: ([解答を表示する](#))

最新問題: 409

IS監査人は、トランザクションを削除する新しいプロセスが悪影響を及ぼさないことの保証を求めている。データベースの整合性への影響。これは、以下の点を分析することで最も効果的に達成できます。

- A. データベース構造。
- B. トリガーの設計。
- C. テスト環境におけるプロセスの結果。
- D. データベースのエンティティ関係図。

Answer: D ([メッセージを残す](#))

セクション：情報資産の保護

最新問題: 410

An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

- A. Obtain senior management sponsorship.
- B. Identify business needs.
- C. Conduct a paper test.
- D. Perform a system restore test.

Answer: C ([メッセージを残す](#))

A best practice would be to conduct a paper test. Senior management sponsorship and business needs identification should have been obtained prior to implementing the plan. A paper test should be conducted first, followed by system or full testing.

最新問題: 411

組織のデータバックアップおよび復元手順を見直す際に、最も重要な考慮事項は次のうちどれですか？

- A. 事業継続計画 (BCP)
- B. リカバリポイント目標 (RPO)
- C. 平均復旧時間 (MTTR)
- D. 平均故障間隔 (MTBF)

Answer: B ([メッセージを残す](#))

説明

リカバリポイント目標 (RPO) とは、予期せぬデータ損失事故発生後に許容される最大データ損失量を時間で表したものです。これは一般的に、事故発生前の時点でデータが正常に復旧できる時点、つまり、最後に取得された信頼性の高いバックアップから経過した時間と考えられています。

RPO（復旧目標時点は、組織のデータバックアップおよび復旧手順を見直す際に考慮すべき重要な要素です。なぜなら、RPOによって、組織がバックアップを実行する頻度や、災害発生時に許容できるデータ損失量が決まるためです。RPOは通常、データのビジネスへの影響度と重要度、およびコンプライアンスや規制要件に基づいて定義されます。例えば、金融機関では取引データに対して非常に低いRPO（数分または数秒など）を設定する一方、研究機関では実験データに対してより高いRPO（数時間または数日など）を設定する場合があります。

その他の選択肢は以下のとおりです。

A：事業継続計画(BCP) BCPとは、組織が混乱や災害が発生した場合に、どのように事業を継続し、重要な機能やプロセスを再開するかを概説した文書です。

BCP（事業継続計画）には、リスク評価、事業影響度分析、復旧戦略、役割と責任、コミュニケーション計画、テストとメンテナンスなど、さまざまな要素が含まれます。BCPは組織が定めたデータバックアップおよび復旧手順と関連していますが、それらを見直す際に最も重要な要素ではありません。BCPは組織全体の復旧目標と戦略を定義するものであり、データバックアップおよび復旧手順はより具体的で技術的な性質のものです。

C：平均復旧時間MTTR）MTTRは、障害や停止後にシステムやサービスを復旧させるのにかかる平均時間を測定する指標です。MTTRは、組織の復旧プロセスの効率性と有効性、およびシステムやサービスの可用性と信頼性を示す指標となります。MTTRは組織が定めたデータバックアップおよび復元手順に関連する指標ですが、それらを評価する際に最も重要な要素ではありません。MTTRは実際の復旧プロセスのパフォーマンスを反映するものであり、データバックアップおよび復元手順は復旧プロセスにおける想定される手順とアクションを定義するものです。

D：平均故障間隔MTBF）MTBFは、システムまたはサービスの故障または停止の平均間隔を測定する指標です。MTBFは、組織のシステムまたはサービスの品質と耐久性、および故障または停止に対する脆弱性を示す指標です。MTBFは、組織が定義したデータバックアップおよび復元手順に関連していますが、それらをレビューする際に考慮すべき最も重要な要素ではありません。MTBFは故障または停止の潜在的な頻度を反映する一方、データバックアップおよび復元手順は、故障または停止に対する緊急時対応計画を定義します。

最新問題: 412

組織の戦略的IT計画をレビューする際、IS監査担当者は以下の点を想定すべきである。

- A. 組織のアプリケーションポートフォリオがビジネス目標に適合しているかどうかの評価。
- B. ハードウェア調達コストを削減するための対策。
- C. 承認されたIT契約リソースのサプライヤーのリスト。
- D. 組織のネットワーク境界セキュリティの技術アーキテクチャの説明。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

組織のアプリケーションポートフォリオが組織のビジネス目標をどの程度サポートしているかを評価することは、IT戦略計画プロセス全体の重要な要素です。これはIT計画の需要側を推進し、一連の戦略的なIT意図に変換されるべきです。その後、アプリケーション、インフラストラクチャ、サービス、管理プロセスなどを含むIT組織全体がビジネス目標をどの程度サポートできるかをさらに評価することができます。運用効率化イニシアチブは、戦略計画ではなく戦術計画に属します。IT戦略計画の目的は、組織のビジネス目標を達成またはサポートするためにITがどのように使用されるかを示すことです。承認されたIT契約リソースのサプライヤーのリストは、戦略的な懸念ではなく、戦術的な懸念です。IT戦略計画には通常、特定の技術アーキテクチャの詳細を含めることはありません。

最新問題: 413

Which of the following statement INCORRECTLY describes network device such as a Router?

- A. Router creates a new header for each packet
- B. Router builds a routing table based on MAC address
- C. Router does not forward broadcast packet
- D. Router assigns a different network address per port

Answer: B ([メッセージを残す](#))

Explanation/Reference:

The INCORRECTLY keyword is used in the question. You need to find out a statement which is not valid about router. Router builds a routing table based on IP address and not on MAC address.

Difference between Router and Bridge:

Router

Bridge

Creates a new header for each packet

Does not alter header. Only reads the header

Builds routing table based on IP address

Build forwarding table based on MAC address

Assigns a different network address per port

Use the same network address for all ports

Filters traffic based on IP address

Filter traffic based on MAC address

Does not forward broadcast packet

Forward broadcast packet

Does not forward traffic that contain destination address unknown to the router Forward traffic if destination address is unknown to bridge For your exam you should know below information about network devices:

Repeaters

A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.

A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

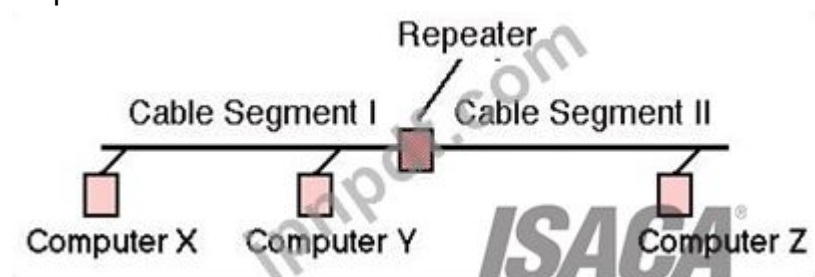


Image from: <http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif> Bridges A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

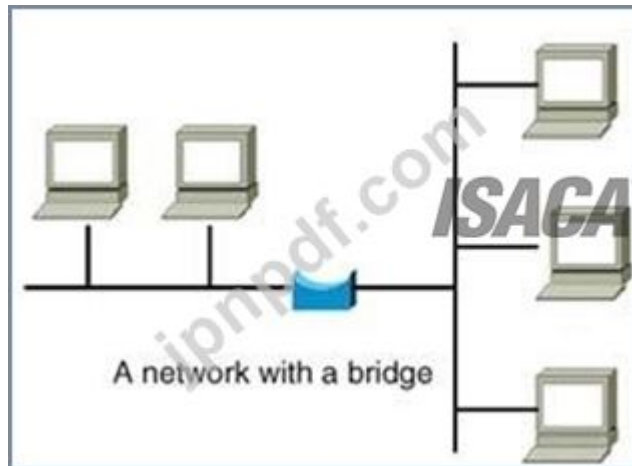


Image from: <http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg>

Routers Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch



Image from: <http://www.computer-networking-success.com/images/router-switch.jpg>

Switches Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions.

Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

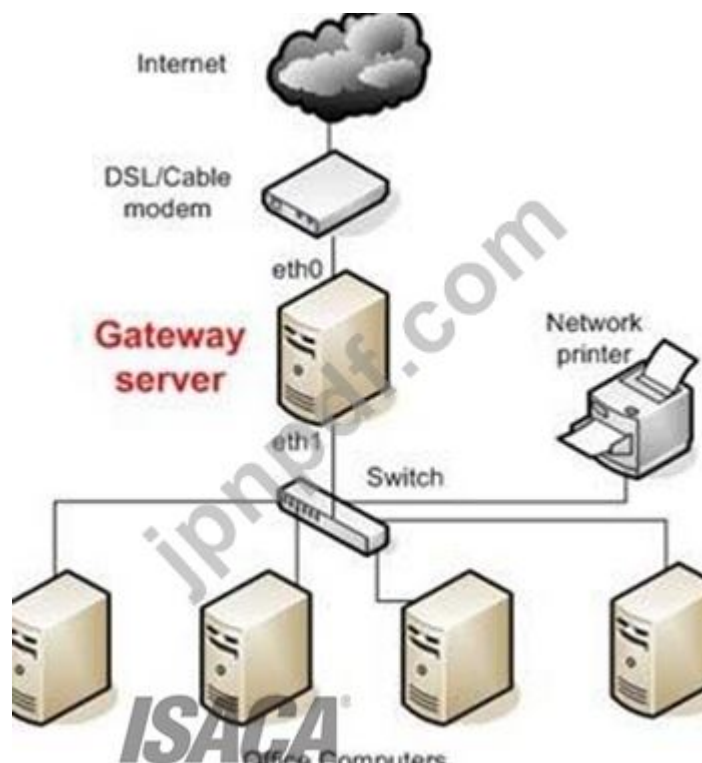


Image from: <http://static.howtoforge.com/>

The following were incorrect answers:

The other options presented correctly describes about Router.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 263

最新問題: 414

アプリケーションシステムの合意されたサービスレベルが満たされていることを示す最良の指標は次のうちどれですか？

- A. トランザクション応答時間
- B. 帯域幅使用状況ログ
- C. セキュリティインシデントレポート
- D. CPU使用率レポート

Answer: C ([メッセージを残す](#))

最新問題: 415

導入後レビューに最も含まれる可能性が高いのは次のうちどれですか？

- A. 現在のテストデータセット
- B. テスト結果
- C. ライブ処理の結果
- D. 開発方法論

Answer: ([解答を表示する](#))

最新問題: 416

システム開発ライフサイクル (SDLC) のどのフェーズで、情報システム監査担当者は、システム仕様に統制が組み込まれていることを確認すると予想するでしょうか？

- A. 実装
- B. デザイン
- C. 開発
- D. 実現可能性

Answer: A ([メッセージを残す](#))

最新問題: 417

In an EDI process, the device which transmits and receives electronic documents is the:

- A. communications handler.
- B. EDI translator.
- C. application interface.
- D. EDI interface.

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

最新問題: 418

Which of the following should be an IS auditor's GREATEST concern when a data owner assigns an incorrect classification level to data?

- A. Controls to adequately safeguard the data may not be applied.
- B. Data may not be encrypted by the system administrator.
- C. Competitors may be able to view the data.
- D. Control costs may exceed the intrinsic value of the IT asset.

Answer: A ([メッセージを残す](#))

The answer A is correct because the greatest concern for an IS auditor when a data owner assigns an incorrect classification level to data is that controls to adequately safeguard the data may not be applied. Data classification is the process of categorizing data assets based on their information sensitivity and business impact. Data classification helps organizations to identify, protect, and manage their data according to their value and risk. Data owners are the individuals or entities who have the authority and responsibility to define, classify, and control the access and use of their data.

Data classification typically involves assigning labels or tags to data assets, such as public, internal, confidential, or restricted. These labels indicate the level of protection and handling required for the data.

Based on the data classification, organizations can implement appropriate controls to safeguard the data, such as encryption, access control lists, audit logs, backup policies, etc. These controls help to prevent unauthorized access, disclosure, modification, or loss of data, and to ensure compliance with relevant laws and regulations.

If a data owner assigns an incorrect classification level to data, it can result in either underprotection or overprotection of the data. Underprotection means that the data is classified at a lower level than it should be, which exposes it to higher risks of compromise or breach. For example, if a data owner classifies personal health information (PHI) as public instead of confidential, it may allow anyone to access or share the data without proper authorization or consent. This can violate the privacy rights of the

data subjects and the compliance requirements of regulations such as HIPAA (Health Insurance Portability and Accountability Act).

Overprotection means that the data is classified at a higher level than it should be, which limits its availability or usability. For example, if a data owner classifies marketing materials as restricted instead of public, it may prevent potential customers or partners from accessing or viewing the data. This can reduce the business value and opportunities of the data.

Therefore, an IS auditor should be concerned about the accuracy and consistency of data classification by data owners, as it affects the security and efficiency of data management. An IS auditor should review the policies and procedures for data classification, verify that the data owners have adequate knowledge and skills to classify their data, and test that the data classification labels match with the actual sensitivity and impact of the data.

References:

- * Data Classification: What It Is and How to Implement It
- * What Is Data Classification? - Definition, Levels & Examples ...
- * Data Classification: A Guide for Data Security Leaders

最新問題: 419

新しいリスク管理プログラムを作成する際には、以下の点を考慮することが極めて重要です。

- A. コンプライアンス対策。
- B. 資源利用
- C. リスク許容度
- D. リスク軽減技術。

Answer: ([解答を表示する](#))

最新問題: 420

IS監査担当者が、組織の重要システムの脆弱性スキャン結果をレビューしている。

脆弱性が修復されたことを検証する最良の方法はどれですか？

- A. パッチ管理に関するドキュメントを確認する。
- B. 是正措置のために変更管理文書を確認する。
- C. 脆弱性スキャンシステムの所有者にインタビューして証拠を入手する。
- D. 脆弱なシステムを再スキャンします。

Answer: ([解答を表示する](#))

最新問題: 421

システム開発プロジェクトにおいて、以下の活動のうちどれに参加すると、IS監査人の独立性が損なわれるでしょうか？

- A. 変換が必要なレポートを推奨する
- B. 毎週開催されるプロジェクト管理チームのプレゼンテーションに参加する
- C. 自動制御に関する設計上の決定を行う
- D. 各プログラム仕様のレビュープロセス

Answer: ([解答を表示する](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 422

通常、LAN管理者は以下のことが制限されます。

- A. エンドユーザーとしての責任を負う。
- B. エンドユーザーマネージャーに報告する。
- C. プログラミングの責任を担う。
- D. LANセキュリティ管理を担当する。

Answer: C ([メッセージを残す](#))

A LAN administrator should not have programming responsibilities but may have end- user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

最新問題: 423

外国におけるサイバーセキュリティ規制への組織の準拠状況を監査する際に、最も役立つのは次のうちどれですか？

- A. 監査の優先順位を、最も運用リスクの高い国に絞る。
- B. 最も厳しい要件を持つ国のサイバーセキュリティ規制に従う。
- C. 各国の監査チームによる調査結果報告を標準化するテンプレートを作成する。
- D. さまざまな規制要件を組織のITガバナンスフレームワークにマッピングする

Answer: ([解答を表示する](#)**)**

説明

外国におけるサイバーセキュリティ規制への組織のコンプライアンス監査を計画する際に最も有効な方法は、さまざまな規制要件を組織のITガバナンスフレームワークにマッピングすることです。これは、ITガバナンスフレームワークが、組織内でITガバナンスを実装、管理、報告するために組織が使用する方法を定義するロードマップであるためです1。ITガバナンスは、堅牢で正式なフレームワークを使用して、ビジネス戦略とIT戦略を整合させるのに役立ちます2。さまざまな規制要件をITガバナンスフレームワークにマッピングすることで、監査人は次のことが可能になります。

組織が各国で事業を行う際に適用される、さまざまなサイバーセキュリティ規制の共通点と相違点を特定する。

各規制要件に照らして、組織のITガバナンス慣行の遵守レベルと成熟度を評価する。

規制要件のいずれかを遵守しない場合、または部分的にしか遵守しない場合に関連するリスクとギャップを評価する。

組織のITガバナンスとサイバーセキュリティ体制を強化するための適切な対策または改善策を提案する。

選択肢Dが正解です。なぜなら、さまざまな規制要件を組織のITガバナンスフレームワークにマッピングすることは、外国におけるサイバーセキュリティ規制への準拠監査を計画および実施するための体系的かつ効果的な方法だからです。

最新問題: 424

特定の脅威に対する全体的なビジネスリスクは、次のように表現できます。

- A. 脅威が脆弱性を悪用することに成功した場合の影響の確率と大きさの積。

- B. 脅威の発生源が脆弱性を悪用することに成功した場合の影響の大きさ。
- C. 特定の脅威源が特定の脆弱性を悪用する可能性。
- D. リスク評価チームの総合的な判断。

Answer: ([解答を表示する](#))

セクション：情報資産の保護

Explanation:

選択肢Aは、影響の可能性と規模を考慮しており、資産に対するリスクを最も適切に評価できます。選択肢Bは、脅威が資産の脆弱性を悪用する可能性のみを示し、資産への損害の規模は示しません。同様に、選択肢Cは損害の規模のみを考慮し、脅威が脆弱性を悪用する可能性は考慮しません。

選択肢Dは、リスクを恣意的な基準で定義しており、科学的なリスク管理プロセスには適していません。

最新問題: 425

組織ネットワーク内での不正行為を検出するための最も効果的な対策は次のとおりです。

- A. 侵入検知システム (IDS)を導入する
- B. 二段階認証を適用する
- C. アクセスログを確認する
- D. 職務分担

Answer: C ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 426

Which of the following is the PRIMARY advantage of using an automated security log monitoring tool instead of conducting a manual review to monitor the use of privileged access?

- A. Ease of log retrieval for audit purposes
- B. Reduced costs associated with automating the review
- C. Ease of storing and maintaining log file
- D. Increased likelihood of detecting suspicious activity

Answer: ([解答を表示する](#))

最新問題: 427

Which of the following approaches will ensure recovery time objectives (RTOs) are met for an organization's disaster recovery plan (DRP)?

- A. Performing a cyber-resilience test
- B. Performing a table top test
- C. Performing a parallel test
- D. Performing a full interruption test

Answer: D ([メッセージを残す](#))

最新問題: 428

組織の災害復旧計画 (DRP)における復旧時間目標 (RTO)の達成を確実にするアプローチは、次のうちどれでしょうか？

- A. 卓上テストの実施
- B. サイバーレジリエンステストの実施
- C. 並列テストの実行
- D. 完全中断テストの実施

Answer: C ([メッセージを残す](#))

最新問題: 429

ある組織は、パイロットリリースを廃止し、すべての機能を単一のリリースで提供する計画を立てています。このアプローチにおける最大のリスクは次のうちどれですか？

- A. プロジェクトを追跡するための監視強化が必要
- B. 時間の経過とともにスコープクリープが発生する可能性
- C. 重大な欠陥を生産に導入する
- D. プロジェクトコストを追跡できない

Answer: C ([メッセージを残す](#))

最新問題: 430

組織がリスク許容度を高めた場合、次のうちどれが最も増加する可能性が高いでしょうか？

- A. セキュリティインシデント
- B. 機会
- C. キー操作
- D. 監査結果

Answer: B ([メッセージを残す](#))

最新問題: 431

組織のインシデント管理プロセスの設計を評価するIS監査担当者にとって、以下のうちどれが最も懸念されるのでしょうか？

- A. サービス管理基準が遵守されていません。
- B. 優先順位付けの基準が定義されていません。
- C. インシデント解決までの予想時間は明記されていません。
- D. 指標は上級管理職に報告されません。

Answer: C ([メッセージを残す](#))

最新問題: 432

次のうち、アクティブなインターネット攻撃を検出するための図として機能するものはどれですか？

- A. ハニーポット
- B. ファイアウォール
- C. 落とし戸
- D. 交通分析

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

Honeypots are computer systems that are expressly set up to attract and trap individuals who attempt to penetrate other individuals' computer systems. The concept of a honeypot is to learn from intruder's actions. A properly designed and configured honeypot provides data on methods used to attack systems.

The data are then used to improve measures that could curb future attacks. A firewall is basically a preventive measure.

Trapdoors create a vulnerability that provides an opportunity for the insertion of unauthorized code into a system. Traffic analysis is a type of passive attack.

最新問題: 433

オープンソース製品を導入する際に、最も重視すべき事項は次のうちどれですか？

- A. 使いやすさ
- B. サポート
- C. 機密保持
- D. パフォーマンス

Answer: B ([メッセージを残す](#))

最新問題: 434

給与計算アプリケーションに関する監査結果を受けて、経営陣は新たな自動化された統制を導入しました。IS監査人がこの新しい統制の有効性を評価する際に、最も役立つのは次のうちどれでしょうか？

- A. 実施前に承認されたテストスクリプトと結果
- B. プロセスと管理を定義する文書化された手順
- C. 承認済みプロジェクト範囲文書
- D. 卓上運動の結果のレビュー

Answer: ([解答を表示する](#))

説明

新しい自動化された制御の有効性を評価する最良の方法は、プロセスと制御を定義する文書化された手順を確認することです。これにより、IS監査担当者は、制御の目的、範囲、役割、責任、および期待される結果を理解できます。文書化された手順は、制御をテストし、監査結果の推奨事項への準拠を確認するための基礎にもなります。参考文献：

ISACAフレームワーク：成功への青写真

CISA試験対策マニュアル（デジタル版）

最新問題: 435

Which of the following is MOST important to include when developing an organization's test strategy?

- A. Risks and contingencies
- B. Test scenario benchmarks
- C. Programming walk-throughs
- D. Results of regression test

Answer: A ([メッセージを残す](#))

The most important aspect to include when developing an organization's test strategy is identifying risks and contingencies. This allows for proactive planning to address potential issues during testing, ensuring that the strategy accounts for unforeseen challenges and has appropriate mitigation measures in place to minimize disruption.

最新問題: 436

ハブとは、以下のものを接続するデバイスです。

- A. 異なるプロトコルを使用する2つのLAN。
- B. WANを備えたLAN。
- C. メトロポリタンエリアネットワーク (MAN)を備えたLAN。
- D. 単一のLANの2つのセグメント。

Answer: D ([メッセージを残す](#))

ハブとは、単一のLAN内の2つのセグメントを接続するデバイスです。ハブはリピーターの種類であり、同じLAN内のすべてのセグメントのユーザーに透過的な接続を提供します。ハブはレベル1デバイスです。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 437

経営情報システム (MIS) をレビューする際に、情報システム監査人が検証すべき最も重要な項目は次のうちどれですか？

- A. データ品質
- B. データアクセス
- C. バックアップ周波数
- D. システムパフォーマンス

Answer: ([解答を表示する](#))

最新問題: 438

During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

- A. be subject to adequate quality assurance (QA).
- B. incorporate changes to relevant laws.
- C. reflect current practices.
- D. include new systems and corresponding process changes.

Answer: C ([メッセージを残す](#))

最新問題: 439

An organization considers implementing a system that uses a technology that is not in line with the organization's IT strategy. Which of the following is the BEST justification for deviating from the IT strategy?

- A. The business benefits are achieved even with extra costs.
- B. The organization has staff familiar with the technology.

- C. The system has a reduced cost of ownership.
- D. The system makes use of state-of-the-art technology.

Answer: C ([メッセージを残す](#))

最新問題: 440

ITプロジェクトのどのフェーズで、ベネフィット実現分析を実施するのが最も適切ですか？

- A. ユーザー受け入れテスト (UAT) フェーズ
- B. 設計レビュー段階
- C. 導入後レビュー段階
- D. 最終実装段階

Answer: ([解答を表示する](#))

最新問題: 441

継続的監査アプローチの利点は、多数のトランザクションを処理するタイムシェアリング環境で使用する場合に、システムセキュリティを向上させることができる点である。正誤を答えよ。

- A. 真
- B. 偽

Answer: ([解答を表示する](#))

説明／参考資料：

確かに、継続的な監査アプローチの利点の一つは、多数のトランザクションを処理するタイムシェアリング環境で使用する場合に、システムセキュリティを向上させることができる点である。

最新問題: 442

ほとんどのITサービスが外部委託されている環境において、事業継続計画を最も適切に管理する方法は次のとおりです。

- A. IT管理、
- B. 経営管理
- C. 事業継続計画の専門家。
- D. アウトソーシングサービスプロバイダーの管理

Answer: C ([メッセージを残す](#))

最新問題: 443

2社間の相互災害復旧協定の監査において、IS監査担当者が最も懸念するのは次の点である。

- A. 緊急時の資源配分。
- B. ハードウェアとソフトウェアの互換性の維持。
- C. ISポリシーと手順の違い。
- D. システムテストの頻度。

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

最新問題: 444

義務付けられた年次セキュリティ意識向上トレーニングの効果を最もよく示す証拠となるのは、次のうちどれでしょうか？

- A. ソーシャルエンジニアリングテスト結果の傾向
- B. 無作為に選ばれた従業員が回答したアンケート
- C. セキュリティインシデント件数
- D. 第三者による侵入テストの結果

Answer: B ([メッセージを残す](#))

最新問題: 445

Which of the following would BEST enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy?

- A. Mobile device tracking program
- B. Mobile device upgrade program
- C. Mobile device testing program
- D. Mobile device awareness program

Answer: ([解答を表示する](#))

A mobile device awareness program would best enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy. A mobile device awareness program is a set of activities that aim to educate and inform the employees about the benefits, challenges, and best practices of using their personal mobile devices for work purposes. A mobile device awareness program can help the organization to:

- * Communicate the organization's policies and expectations regarding BYOD, such as which devices are allowed, what data can be accessed or stored, and what security measures are required.
- * Raise the employees' awareness of the potential threats and vulnerabilities that affect their mobile devices, such as malware, phishing, data leakage, or device loss.
- * Provide the employees with guidance and tips on how to protect their mobile devices and the organization's data, such as using strong passwords, encryption, antivirus software, remote wipe, or VPN.
- * Encourage the employees to report any incidents or issues related to their mobile devices, such as suspicious messages, unauthorized access, or device damage.

A mobile device awareness program can help the organization to reduce the security risks associated with BYOD by enhancing the employees' knowledge, skills, and behavior in using their mobile devices securely and responsibly. A mobile device awareness program can also help the organization to comply with relevant regulations and standards that govern data privacy and security in the cloud¹.

The other options are not as effective as a mobile device awareness program in enabling an organization to address the security risks associated with BYOD. Option A, mobile device tracking program, is a tool that allows the organization to monitor and locate the employees' mobile devices in case of loss or theft. However, this tool may not prevent or detect other types of security risks, such as malware infection or data breach.

Option B, mobile device upgrade program, is a process that ensures that the employees' mobile devices are running the latest versions of operating systems and applications. However, this process may not address other aspects of security, such as user behavior or data protection. Option C, mobile device testing program, is a method that verifies the functionality and compatibility of the employees' mobile devices with the organization's systems and networks. However, this method may not cover all the scenarios or factors that may affect the security of the mobile devices or the organization's data².

References:

* Mobile Device Security Awareness Topics3

* Security Awareness Top Ten Topics - #8 Mobile Devices

最新問題: 446

ISセキュリティポリシーの策定に関して、最終的な責任は誰にあるのでしょうか？

- A. 取締役会
- B. 中間管理職
- C. セキュリティ管理者
- D. ネットワーク管理者

Answer: A ([メッセージを残す](#))

説明／参考資料：

取締役会は、情報セキュリティポリシーの策定について最終的な責任を負う。

最新問題: 447

組織の災害復旧計画（DRP）をレビューする情報システム監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？

- A. DRPは経営陣によって正式に承認されていません。
- B. DRPはエンドユーザーに配布されていません。
- C. DRPはITインフラストラクチャのアップグレード以降更新されていません。
- D. DRPには、重要なサーバーのみの復旧手順が含まれています。

Answer: C ([メッセージを残す](#))

組織の災害復旧計画（DRP）をレビューする情報システム監査担当者にとって最大の懸念事項は、ITインフラストラクチャのアップグレード以降、DRPが更新されていないことです。これは、DRPがITシステムの現在の構成、依存関係、または復旧要件を反映していない可能性があるため、DRPが時代遅れまたは無効になる原因となります。情報システム監査担当者は、IT環境の変化に合わせてDRPが定期的にレビューされ、更新されていることを確認する必要があります。DRPが経営陣によって正式に承認されていないことは、組織のDRPをレビューする情報システム監査担当者にとって懸念事項ですが、DRPが最新かつ有効であることを確認することほど重要ではありません。DRPがエンドユーザーに配布されていない、またはDRPに重要なサーバーの復旧手順のみが含まれているといった問題は、DRPの有効性や効果ではなく、DRPの伝達または範囲に関する問題です。参考文献：

ISACA、CISAレビューマニュアル、第27版、2018年、389ページ

最新問題: 448

What type of approach to the development of organizational policies is often driven by risk assessment?

- A. Bottom-up
- B. Top-down
- C. Comprehensive
- D. Integrated

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

A bottom-up approach to the development of organizational policies is often driven by risk assessment.

最新問題: 449

An IS auditor reviewing database security should be MOST concerned if the database administrator (DBA):

- A. approves access roles
- B. resolves database locks
- C. executes recovery procedures
- D. assesses database performance

Answer: A ([メッセージを残す](#))

Allowing the DBA to both manage the database and approve user access roles concentrates too much power in one role. This violates the principle of segregation of duties and increases the risk of unauthorized or inappropriate access going undetected.

最新問題: 450

An IS auditor finds ad hoc vulnerability scanning is in place with no clear alignment to the organization's wider security threat and vulnerability management program. Which of the following would BEST enable the organization to work toward improvement in this area?

- A. Outsourcing the threat and vulnerability management function to a third party
- B. Implementing security logging to enhance threat and vulnerability management
- C. Using a capability maturity model to identify a path to an optimized program
- D. Maintaining a catalog of vulnerabilities that may impact mission-critical systems

Answer: C ([メッセージを残す](#))

最新問題: 451

In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- A. Nonrepudiation
- B. Encryption
- C. Authentication
- D. Integrity

Answer: ([解答を表示する](#))

Nonrepudiation , achieved through the use of digital signatures, prevents the claimed sender from later denying that they generated and sent the message. Encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made. Authentication is necessary to establish the identification of all parties to a communication. Integrity ensures that

transactions are accurate but does not provide the identification of the customer.

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 452

ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?

- A. Reliability
- B. Usability
- C. Functionality
- D. Maintainability

Answer: C ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties.

The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

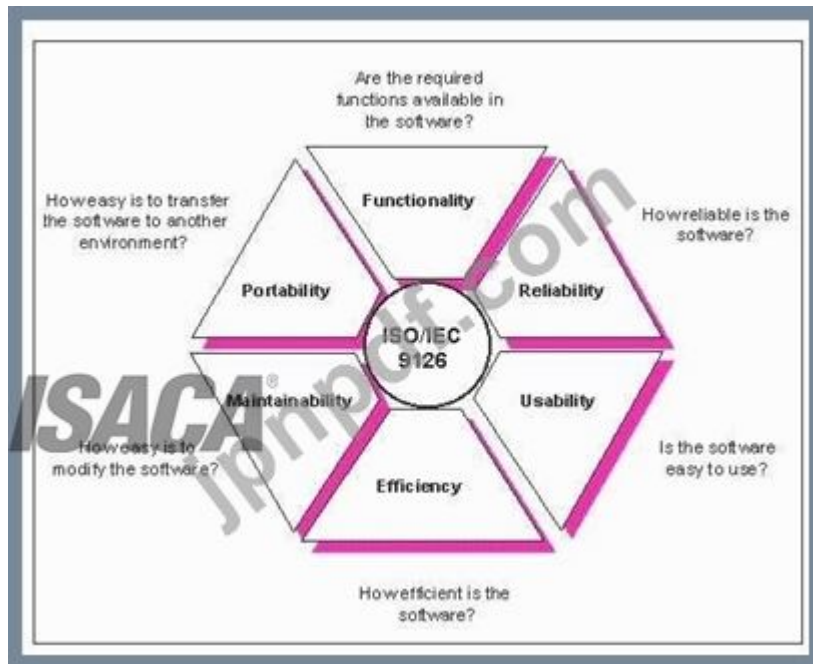
Functionality Compliance

For CISA Exam you should know below information about ISO 9126 model:

ISO/IEC 9126 Software engineering - Product quality was an international standard for the evaluation of software quality. It has been replaced by ISO/IEC 25010:2011.[1] The fundamental objective of the ISO/IEC

9126 standard is to address some of the well-known human biases that can adversely affect the delivery and perception of a software development project. These biases include changing priorities after the start of a project or not having any clear definitions of "success." By clarifying, then agreeing on the project priorities and subsequently converting abstract priorities (compliance) to measurable values (output data can be validated against schema X with zero intervention), ISO/IEC 9126 tries to develop a common understanding of the project's objectives and goals.

ISO 9126



The standard is divided into four parts:

Quality model

External metrics

Internal metrics

Quality in use metrics.

Quality Model

The quality model presented in the first part of the standard, ISO/IEC 9126-1,[2] classifies software quality in a structured set of characteristics and sub-characteristics as follows:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

Functionality Compliance

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Maturity

Fault Tolerance

Recoverability

Reliability Compliance

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

Understandability

Learn ability

Operability

Attractiveness

Usability Compliance

Efficiency - A set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.

Time Behavior

Resource Utilization

Efficiency Compliance

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

Analyzability

Changeability

Stability

Testability

Maintainability Compliance

Portability - A set of attributes that bear on the ability of software to be transferred from one environment to another.

Adaptability

Install ability

Co-Existence

Replace ability

Portability Compliance

Each quality sub-characteristic (e.g. adaptability) is further divided into attributes. An attribute is an entity which can be verified or measured in the software product. Attributes are not defined in the standard, as they vary between different software products. Software product is defined in a broad sense: it encompasses executables, source code, architecture descriptions, and so on. As a result, the notion of user extends to operators as well as to programmers, which are users of components such as software libraries.

The standard provides a framework for organizations to define a quality model for a software product. On doing so, however, it leaves up to each organization the task of specifying precisely its own model. This may be done, for example, by specifying target values for quality metrics which evaluates the degree of presence of quality attributes.

Internal Metrics

Internal metrics are those which do not rely on software execution (static measure) External Metrics External metrics are applicable to running software.

Quality in Use Metrics

Quality in use metrics are only available when the final product is used in real conditions.

Ideally, the internal quality determines the external quality and external quality determines quality in use.

This standard stems from the GE model for describing software quality, presented in 1977 by McCall et al., which is organized around three types of Quality Characteristics:

Factors (To specify): They describe the external view of the software, as viewed by the users.

Criteria (To build): They describe the internal view of the software, as seen by the developer.

Metrics (To control): They are defined and used to provide a scale and method for measurement.

ISO/IEC 9126 distinguishes between a defect and a nonconformity, a defect being The nonfulfillment of intended usage requirements, whereas a nonconformity is The nonfulfillment of specified requirements. A similar distinction is made between validation and verification, known as V&V in the testing trade.

The following were incorrect answers:

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

Reference:

CISA review manual 2014 Page number 188

最新問題: 453

データウェアハウス (DW) 管理において、ソースシステムからの変更によって引き起こされるデータ品質の問題を防止するための最善の方法は何ですか？

- A. データウェアハウスとソースシステム間の差異をチェックするためのデータ品質アラートを設定します。
- B. 2つのシステム間の抽出/転送/ロード (ETL) プロセスの変更には承認が必要
- C. データウェアハウスを影響分析に含める またはソースシステムへの変更を含める)
- D. 2つのシステム間での抽出/転送/ロード (ETL) プロセスの変更へのアクセスを制限する

Answer: C ([メッセージを残す](#))

ソースシステムの変更に伴うデータ品質問題を防止する最善の方法は、ソースシステムの変更の影響分析にデータウェアハウスを含めることです。データウェアハウスは、1つまたは複数のソースシステムからの統合データを一元管理するリポジトリです。影響分析とは、既存のシステムまたは環境に対する変更の潜在的な影響と結果を評価する手法です。影響分析にデータウェアハウスを含めることで、ソースシステムの変更によって発生する可能性のあるデータ品質問題 (データの不整合、不完全性、不正確性など) を特定し、軽減することができます。その他の方法は、データ品質アラート、変更の承認、アクセス制限などを伴う場合があります。そのため、データ品質問題を防止する効果は劣ります。参考文献:

* CISAレビューマニュアル (デジタル版)、第5章、セクション5.41

* CISA復習問題、解答、解説データベース、問題ID 226

最新問題: 454

FTP経由でのファイルのダウンロードを制御する効果的な方法は次のうちどれですか？最も適切な回答を選択してください。

- A. アプリケーション層ゲートウェイ、またはプロキシファイアウォールであり、ステートフルインスペクションファイアウォールではない。
- B. アプリケーション層ゲートウェイ、またはプロキシファイアウォール
- C. 回路レベルのゲートウェイ
- D. 第一世代のパケットフィルタリングファイアウォール

Answer: B ([メッセージを残す](#))

アプリケーション層ゲートウェイ、またはプロキシファイアウォールは、FTPによるファイルのダウンロードを制御する効果的な方法です。FTPはOSI参照モデルのアプリケーション層プロトコルであるため、最も効果的なファイアウォールは、アプリケーション層を通して検査できる必要があります。

最新問題: 455

ウェブサーバー上で共通ゲートウェイインターフェース (CGI) が最もよく使用されるのはどのような場合ですか？

- A. アプリケーションプログラムとユーザー間でデータを転送するための統一された方法

- B. 映画やテレビ向けのコンピュータグラフィックス画像処理方法
- C. ウェブデザインのためのグラフィカルユーザーインターフェース
- D. プライベートゲートウェイドメインにアクセスするためのインターフェース

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

共通ゲートウェイインターフェース (CGI)は、Webサーバーがユーザーのリクエストをアプリケーションプログラムに渡し、ユーザーとの間でデータをやり取りするための標準的な方法です。ユーザーがWebページをリクエストすると た例えば、Webサイトのアドレスを示すハイライトされた単語をクリックするなど)、サーバーはリクエストされたページを返します。しかし、ユーザーがWebページ上のフォームに入力して送信すると、通常はアプリケーションプログラムによる処理が必要になります。Webサーバーは通常、フォーム情報を小さなアプリケーションプログラムに渡し、そのプログラムがデータを処理し、確認メッセージを返す場合があります。サーバーとアプリケーション間でデータをやり取りするためのこの方法、または慣習は、共通ゲートウェイインターフェース (CGI)と呼ばれます。これはWebのHTTPプロトコルの一部です。

最新問題: 456

Which of the following provides the GREATEST assurance of message authenticity?

- A. The prehash code is derived mathematically from the message being sent.
- B. The prehash code is encrypted using the sender's private key.
- C. The prehash code and the message are encrypted using the secret key.
- D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Answer: B ([メッセージを残す](#))

Encrypting the prehash code using the sender's private key provides assurance of the authenticity of the message.

Mathematically deriving the prehash code provides integrity to the message. Encrypting the prehash code and the message using the secret key provides confidentiality.

最新問題: 457

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____ . (fill-in-the-blank)

- A. Security administrator
- B. Systems auditor
- C. Board of directors
- D. Financial auditor

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

最新問題: 458

職務分掌が適切に行われている場合、品質管理担当者が変更管理や問題管理の責任も担うことを妨げるものではない。正誤を答えよ。

- A. 真
- B. 偽

Answer: A ([メッセージを残す](#))

説明／参考資料：

適切な職務分掌は、品質管理担当者が変更管理や問題管理の責任も担うことを妨げるものではない。

最新問題: 459

新しいシステムを並行して運用する主な目的は以下のとおりです。

- A. 包括的なユニットおよびシステムテストの基礎を提供する。
- B. 2つのシステムのうち、どちらがより効率的で効果的かを判断する。
- C. 新システムの動作を前システムと比較して検証する。
- D. プログラムとファイルインターフェースのエラーをすべて解決します。

Answer: C ([メッセージを残す](#))

最新問題: 460

監査報告書を提出した後、監査マネージャーは監査中に証拠が見落とされていたことを発見しました。この証拠は、手続き上の統制が失敗した可能性があり、監査の結論と矛盾する可能性があることを示しています。この見落としによって最も影響を受けるリスクは次のうちどれですか？

- A. 固有の
- B. 監査
- C. 運用中
- D. 金融

Answer: ([解答を表示する](#)**)**

最新問題: 461

バッチ更新ジョブが完了したかどうかを判断するのに最適な方法は次のうちどれですか？

- A. プロセスオーナーの確認を取得する
- B. 脚本のコピーを確認する
- C. ジョブログの確認
- D. トランザクションのサンプルをテストする

Answer: ([解答を表示する](#)**)**

最新問題: 462

IT戦略をビジネス戦略と整合させることは、主に組織にとって以下の点で役立ちます。

- A. IT分野における上級管理職の関与を増やす。
- B. Optimize investments in IT.
- C. Create risk awareness across business units.

D. Monitor the effectiveness of IT.

Answer: B ([メッセージを残す](#))

Comprehensive and Detailed Step-by-Step Explanation:

Aligning IT with business strategy ensures that IT investments provide value and support business objectives.

* Option A (Incorrect): While senior management involvement is essential, it is a byproduct of alignment rather than the primary goal.

* Option B (Correct): The main purpose of alignment is to optimize IT investments by ensuring that IT initiatives directly support business needs, reducing waste and improving ROI.

* Option C (Incorrect): Risk awareness is important but is not the primary reason for IT-business alignment.

* Option D (Incorrect): Monitoring IT effectiveness is part of governance but not the main objective of IT-business alignment.

Reference: ISACA CISA Review Manual - Domain 1: Information Systems Auditing Process- Covers IT governance, strategy alignment, and value realization.

最新問題: 463

組織が統制自己評価 (CSA) 手法を採用することで得られる主な利点は、以下のとおりです。

A. 後で詳細なレビューが必要になる可能性のある高リスク領域を特定できます。

B. IS監査人がリスクを独立して評価できるようにする。

C. 従来の監査の代替として使用できます。

D. 経営陣が管理責任を放棄することを可能にする。

Answer: A ([メッセージを残す](#))

CSAは、直ちに注意を払う必要がある、または後日より徹底的なレビューが必要な高リスク領域のレビューを前提としています。選択肢Bは、CSAには監査担当者とラインマネジメントの関与が必要であるため誤りです。実際には、内部監査機能が統制監視責任の一部を機能領域に移管します。選択肢Cは、CSAが従来の監査の代替ではないため誤りです。CSAは監査の責任を代替することを目的としているのではなく、それを強化することを目的としています。選択肢Dは、CSAが経営陣による統制責任の放棄を認めていないため誤りです。

最新問題: 464

An organization has alternative links in its wide area network (WAN) to provide redundancy.

However, each time there is a problem with a link, network administrators have to update the configuration to divert traffic to the other link. Which of the following would be an IS auditor's BEST recommendation?

A. Reduce the number of alternative links

B. Implement a load-balancing mechanism

C. Configure a non-proprietary routing protocol

D. Implement an exterior routing protocol

Answer: C ([メッセージを残す](#))

標準規格に基づいた動的ルーティングプロトコル（例えばOSPF）を導入することで、ルータはリンクの状態を自動的に検出し、通知することができます。WANリンクが1つ故障した場合、ルーティングテーブルが統合され、手動操作なしにトラフィックがバックアップパスに再ルーティングされるため、シームレスな冗長性が実現します。

最新問題: 465

Which of the following is the GREATEST risk associated with instant messaging?

- A. Data governance may become ineffective.
- B. Data classification procedures may not be followed.
- C. Data logging is more difficult.
- D. Data exfiltration is more likely to occur.

Answer: D ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation/Reference:

最新問題: 466

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- A. Wet-pipe sprinkler system
- B. Dry-pipe sprinkler system
- C. FM-200system
- D. Carbon dioxide-based fire extinguishers

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

FM-200 is safer to use than carbon dioxide. It is considered a clean agent for use in gaseous fire suppression applications. A water-based fire extinguisher is suitable when sensitive computer equipment could be damaged before the fire department personnel arrive at the site. Manual firefighting (fire extinguishers) may not provide fast enough protection for sensitive equipment (e.g., network servers).

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 467

組織の新たに導入されたオンラインセキュリティ意識向上プログラムをレビューするIS監査担当者にとって、以下の調査結果のうちどれが最も懸念すべきでしょうか？

- A. 新入社員のみがプログラムへの参加を義務付けられています。
- B. トレーニング結果を評価するための指標は確立されていません。
- C. 従業員は結果を即座に通知されません
- D. プログラム更新の時期は未定です

Answer: B ([メッセージを残す](#))

説明

オンラインセキュリティ意識向上プログラムをレビューするIS監査担当者にとって最大の懸念事項は、トレーニング結果を評価するための指標が確立されていないことです。指標がなければ、プログラムの効果を測定し、改善すべき領域を特定することは困難です。その他の指摘事項も対処すべき問題ではありますが、指標の欠如ほど重要ではありません。参考文献 :CISAレビューマニュアル (デジタル版)、第〇章
5、セクション5.3.11

最新問題: 468

ある企業が、アプリケーションに保存されている情報が適切に保護されているかどうかを判断するための監査を依頼しました。監査作業を開始する前に、次のうち最も重要な行動はどれですか？

- A. 是正措置報告書を確認する
- B. 管理目標を設定する。
- C. 脅威の状況进行评估する。
- D. 侵入テストを実施する。

Answer: B (メッセージを残す)

監査作業を開始する前に最も重要なことは、統制目標を設定することです。統制目標とは、アプリケーションの情報保護に関して監査が達成または検証しようとする具体的な目標または成果のことです¹。統制目標は、監査手順の設計と実施、監査証拠の評価、監査結果と勧告の報告の基礎となります²。統制目標はまた、監査の範囲と基準をビジネスのニーズと期待に合わせ、監査が関連性があり、信頼性が高く、効率的であることを保証するのにも役立ちます³。

情報保護監査における管理目標の例としては、以下のようなものがあります。

- * アプリケーションに保存される情報が、その機密性、価値、および規制要件に従って分類されることを保証するため
- * アプリケーションに保存される情報が、必要に応じて暗号化、マスキング、または匿名化されることを保証するため
- * アプリケーションに保存されている情報が、許可されたユーザーとプロセスのみによってアクセス可能であることを保証するため
- * アプリケーションに保存されている情報が、事業継続およびデータ保持ポリシーに従ってバックアップ、復元、および保持されることを保証するため
- * アプリケーションに保存されている情報が監視、ログ記録され、不正または異常なアクティビティがないか監査されることを保証するため。したがって、オプション B が正解です。

選択肢Aは正しくありません。なぜなら、是正報告書を確認することは、監査作業開始前に最も重要な行動ではないからです。是正報告書とは、被監査者が過去の監査結果や問題点をどのように解決または対処したかを記述した文書です。是正報告書を確認することは、アプリケーションにおける情報保護の現状を理解する上で役立つかもしれませんが、監査の統制目標を定義するための前提条件ではありません。

選択肢Cは正しくありません。なぜなら、監査作業を開始する前に脅威の状況进行评估することは最も重要な行動ではないからです。脅威の状況とは、アプリケーションに保存されている情報に影響を与える可能性のあるサイバー攻撃やデータ侵害の潜在的な発生源、方法、および影響の集合です⁵。脅威の状況进行评估することは、アプリケーションにおける情報保護のリスクと脆弱性を特定し、優先順位付けするのに役立つかもしれませんが、監査の統制目標を定義するための前提条件ではありません。

選択肢Dは正しくありません。なぜなら、侵入テストの実施は監査作業開始前に最も重要な行動ではないからです。侵入テストとは、現実世界のサイバー攻撃やデータ漏洩をシミュレートして、情報システムやアプリケーションのセキュリティと回復力をテストする手法です。

最新問題: 469

The IS auditor of a power company finds that the radio link to a remote mountain site is experiencing systematic outages under specific weather conditions. The communications manager explains that increasing the radio power would require a new license and would help little. What is the MOST appropriate action by the IS auditor?

- A. Recommend that the site's data collection and transmission be non-interruptible.
- B. Review the installation license, permissions and associated costs.
- C. Recommend that the site's hardware be upgraded to record data during outages.
- D. Gather additional information to identify threats, vulnerabilities, and impact.

Answer: D ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: 470

When auditing an organization's procurement process, which of the following observations should be of MOST concern to an IS auditor?

- A. Thresholds for requesting and approving payments for purchase requests have not been established.
- B. Contracts can be approved after expenses have been incurred.
- C. The procurement manager is new to the organization.
- D. Purchasing procedures and processes have not been updated during the past two years.

Answer: ([解答を表示する](#)**)**

最新問題: 471

次のうち、データに対するセキュリティレベルを向上させるオブジェクト指向技術の特徴はどれですか？

- A. 継承
- B. ダイナミックウェアハウジング
- C. カプセル化
- D. 多型性

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

説明

Explanation:

カプセル化はオブジェクトの特性であり、事前に公開として定義されていないプロパティやメソッドへのアクセスを防止します。つまり、オブジェクトの振る舞いの実装にはアクセスできません。オブジェクトは外部との通信インターフェースを定義し、そのインターフェースに属するものだけがアクセス可能です。

最新問題: 472

組織の情報セキュリティ部門は、裁判で使用する可能性のあるデジタル証拠の取り扱いに関する手順を作成しています。リスクの観点から、以下のうちどれを確実に実施することが最も重要ですか？

- A. 元のデータは機密情報として扱われます。
- B. データの完全性が維持されます
- C. バックアップデータに対して分析を行うことができます

D. 証拠は規制遵守に準拠している

Answer: ([解答を表示する](#))

最新問題: 473

A finance department has a multi-year project to upgrade the enterprise resource planning (ERP) system hosting the general ledger. and in year one, the system version upgrade will be applied. Which of the following should be the PRIMARY focus of the IS auditor reviewing the first year of the project?

- A. unit testing
- B. Network performance
- C. User acceptance testing (UAT)
- D. Regression testing

Answer: ([解答を表示する](#))

The primary focus of the IS auditor reviewing the first year of the project should be regression testing.

Regression testing is a type of testing that ensures that the existing functionality of the system is not affected by the changes or upgrades made to the system. Since the project involves upgrading the ERP system hosting the general ledger, which is a critical and complex component of the finance department, it is important to verify that the upgrade does not introduce any errors or defects that could compromise the accuracy, completeness, and reliability of the financial data and reports. Regression testing can help identify and resolve any issues before they affect the users and the business processes.

Unit testing, network performance, and user acceptance testing (UAT) are also important aspects of the project, but they are not the primary focus of the IS auditor in the first year. Unit testing is a type of testing that verifies that each individual module or component of the system works as expected. Network performance is a measure of how well the system can communicate and exchange data with other systems and devices over a network. User acceptance testing (UAT) is a type of testing that validates that the system meets the user requirements and expectations. These aspects are more relevant in later stages of the project, when the system is more developed and ready for deployment.

References:

ERP Upgrade: The Path to Modernization | SAP

ERP System Validation: Your Guide To Successfully Validating ERP Systems The role of internal auditors in ERP#based organizations What is Regression Testing? Definition, Tools & Examples What is Unit Testing? Definition, Tools & Examples What is Network Performance? Definition, Metrics & Examples What is User Acceptance Testing (UAT)? Definition, Process & Examples

最新問題: 474

Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

- A. format string vulnerabilities
- B. integer overflow
- C. code injection
- D. command injection
- E. None of the choices.

Answer: ([解答を表示する](#))

Section: Protection of Information Assets

Explanation:

Code injection is a technique to introduce code into a computer program or system by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs.

最新問題: 475

What is the primary objective of a control self-assessment (CSA) program?

- A. Enhancement of the audit responsibility
- B. Elimination of the audit responsibility
- C. Replacement of the audit responsibility
- D. Integrity of the audit responsibility

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

最新問題: 476

システム開発スタッフの新規メンバーに付与する場合、以下のアクセス権限のうちどれが最も大きなリスクをもたらしますか？

- A. 生産プログラムライブラリへの書き込みアクセス
- B. 開発データライブラリへの書き込みアクセス
- C. 実稼働プログラムライブラリへのアクセスを実行します
- D. 開発プログラムライブラリへのアクセスを実行します

Answer: A ([メッセージを残す](#))

システム開発スタッフの新メンバーに本番プログラムライブラリへの書き込みアクセス権を付与することは、最も大きなリスクを伴います。本番プログラムライブラリには、稼働中のシステム上で実行され、重要な業務機能を支える実行可能コードが含まれています。書き込みアクセス権があれば、ユーザーは既存のプログラムを変更または削除したり、ライブラリに新しいプログラムを追加したりできます。ユーザーが本番プログラムに不正な変更や誤った変更を加えた場合、組織の業務に深刻な混乱、エラー、またはセキュリティ侵害を引き起こす可能性があります。

したがって、本番環境のプログラムライブラリへの書き込みアクセスは、権限のある担当者だけに制限し、厳格な変更管理の対象とする必要があります。

最新問題: 477

災害発生時に組織のバックアップメディアが十分であることを最も確実に保証できるのは、次のうちどれでしょうか？

- A. バックアップ機器の定期メンテナンス
- B. バックアップログを定期的に確認し、本番環境からのすべてのデータが含まれていることを確認する。
- C. テスト環境における生産システムの定期的復旧
- D. バックアップメディアの読み書きテストをスケジュールする

Answer: ([解答を表示する](#)**)**

最新問題: 478

監査担当者は、月末処理を実行するために管理者ユーザーIDが3人の財務マネージャー間で共有されていることを指摘した。

更新。財務における管理者IDを確実にするための最適な推奨事項は次のうちどれですか。
システムは効果的に制御されていますか？

- A. 個別のソフトウェアトークンの使用を実装する
- B. 従業員の意識向上研修を実施する
- C. 研究所のユーザーIDログ記録と監視
- D. 財務システム内のデータが分類されていることを確認する

Answer: A ([メッセージを残す](#))

セクション：情報システムの監査プロセス

最新問題: 479

ITセキュリティインシデント対応プロセスの事後分析で特定された以下の問題のうち、最も懸念すべきものはどれですか？

- A. 事件の根本原因が適切に特定され、文書化されていなかった
- B. インシデント対応チームメンバーの連絡先情報が最新ではありませんでした。
- C. この事件は、ゼロデイ脆弱性を悪用した攻撃者によって引き起こされました。
- D. インシデント対応チームは、インシデントの影響を限定するための措置を開始しなかった。

Answer: ([解答を表示する](#))

最新問題: 480

IS監査担当者がデータベースのログ設定を確認したところ、データベース内でINSERT操作とDELETE操作のみが監視されていることに気づいた。最も重大なリスクは何か？

- A. 既存の記録の変更は記録されない場合があります。
- B. メタデータはログに記録されない場合があります。
- C. 削除されたレコードはログに記録されない場合があります。
- D. 新しく追加されたレコードは記録されない場合があります。

Answer: A ([メッセージを残す](#))

最新問題: 481

効果的な自己評価 (CSA) プログラムにとって、以下のうち最も重要なものはどれですか？

- A. 評価範囲の決定
- B. 詳細な試験手順の実施
- C. リスク環境の変化の評価
- D. ビジネスプロセスの理解

Answer: D ([メッセージを残す](#))

効果的なコントロール自己評価 (CSA) プログラムにとって、ビジネスプロセスを理解することが最も重要な要素です。CSAプログラムとは、事業部門、機能、またはプロセスに直接関与する管理者や作業チームが、組織のリスク管理およびコントロールプロセスを評価することを可能にする手法です¹。CSAプログラムは、戦略的な事業目標の達成に対するリスクと潜在的な影響を特定し、コントロールの適切性と有効性を評価し、ギャップや弱点に対処するための是正計画を実施するのに役立ちます²。CSAを成功させるには、レビュー対象のビジネスプロセスについて、その目的、インプット、アウトプット、アクティビティ、リソース、依存関係、利害関係者、パフォーマンス指標などを含め、明確かつ包括的に理解することが不可欠です。これにより、プロセスに関連するリスクとコントロールを特定し、その影響と発生可能性を評価することができます。評価の範囲を決定し、詳細なテスト手

順を実行し、リスク環境の変化を評価することも、効果的なCSAプログラムにとって重要な要素ですが、ビジネスプロセスを理解することほど重要ではありません。これらの要素はCSAプログラムの実行および監視フェーズに関係する一方、ビジネスプロセスの理解は計画および準備フェーズに関係します。ビジネスプロセスをしっかりと理解していなければ、CSAの範囲、テスト、および評価は正確または完全ではない可能性があります。参考文献 :ISACA CISAレビューマニュアル第27版、310ページ

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 482

物理的な破壊が現実的でない場合、ハードディスク上の機密データを処分する最も効果的な方法は次のうちどれですか？

- A. 再フォーマット
- B. 複数回上書き
- C. ファイルを順番に削除する
- D. ディスクの暗号化

Answer: ([解答を表示する](#))

最新問題: 483

組織のネットワーク脅威対応プロセスをレビューした際、IS監査担当者は、アラートの大部分が解決されないままクローズされていることに気づいた。

経営陣は、これらのアラートは実行可能な情報が不足しているため機能しないとして、サポートチームがアラートをクローズすることを許可したと回答しました。監査担当者がこの状況に対処する最善の方法は何でしょうか？

- A. 未対応のアラートをさらにレビューして、脅威の不適切な処理を特定します。
- B. 未対応のアラートを再開し、監査委員会に報告する。
- C. 経営陣に対し、ポリシーを強化し、脅威認識トレーニングを改善することを推奨します。
- D. この慣行は現行の方針に準拠しているため、報告書からこの調査結果を削除してください。

Answer: A ([メッセージを残す](#))

最新問題: 484

The risks associated with electronic evidence gathering would MOST likely be reduced by an e- mail:

- A. destruction policy.
- B. security policy.
- C. archive policy.
- D. audit policy.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

最新問題: 485

災害復旧計画 (DRP)には、以下の手順を含める必要があります。

- A. リスクの評価と定量化。
- B. 災害対策コンサルタントとの契約交渉。
- C. アプリケーション制御要件の特定。
- D. 代替品の入手。

Answer: D ([メッセージを残す](#))

説明

災害復旧計画 (DRP)とは、企業の重要資産を概説し、予期せぬ事態への対応方法を説明した、詳細かつ文書化された一連のガイドラインです。予期せぬ事態や災害には、通常、サイバー攻撃、システム障害、停電、自然災害、機器の故障、インフラの損傷などが含まれます¹。DRPは、災害が企業の事業継続性、データの完全性、およびサービス提供に与える影響を最小限に抑えることを目的としています。また、DRPは、組織が災害からできるだけ迅速かつ効率的に復旧できるよう支援します。

災害復旧計画 (DRP)には、代替品の調達手順を含める必要があります。これは、災害後に組織の通常の業務を復旧させる上で不可欠な要素だからです。代替品には、ハードウェア、ソフトウェア、データ、ネットワーク機器、事務機器、その他、災害によって中断された業務機能やプロセスを再開するために必要なリソースが含まれます。代替品の調達には、ベンダー、サプライヤー、パートナーへの連絡、バックアップシステムや代替システムの起動、新規機器の購入またはレンタルなどが含まれる場合があります。DRPでは、代替品の入手先、場所、費用、および調達と設置の手順と責任を明確にする必要があります。

The other three options are not steps that a DRP should include, as they are either part of the pre-disaster planning process or not directly related to the disaster recovery objectives. Assessing and quantifying risk is a step that should be done before creating a DRP, as it helps identify the potential threats and vulnerabilities that could affect the organization and determine the likelihood and impact of each scenario². Negotiating contracts with disaster planning consultants is also a pre-disaster activity that may help the organization design, implement, test, and maintain a DRP with external expertise and guidance³. Identifying application control requirements is not a step in a DRP, but rather a part of the application development and maintenance process that ensures the quality, security, and reliability of the software applications used by the organization.

Therefore, obtaining replacement supplies is the correct answer.

References:

What is a Disaster Recovery Plan? + Complete Checklist

Risk Assessment - ISACA

Disaster Recovery Planning - ISACA

[Application Controls - ISACA]

最新問題: 486

ある組織は、業務目的で個人情報を取得する提案を受けて、顧客向けWebアプリケーションのセキュリティ強化に取り組んでいます。この取り組みを実施する前に、以下のうちどれを最も重要視して確認すべきでしょうか？

- A. 顧客への通知手順
- B. Data ownership assignments

- C. Regulatory compliance requirements
- D. Encryption capabilities

Answer: C ([メッセージを残す](#))

最新問題: 487

During an audit of a multinational bank's disposal process, an IS auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

- A. Backup media are not reviewed before disposal.
- B. Backup media are disposed before the end of the retention period.
- C. Hardware is not destroyed by a certified vendor.
- D. Degaussing is used instead of physical shredding.

Answer: ([解答を表示する](#))

最新問題: 488

Which of the following groups is PRIMARILY accountable for establishing a culture that facilitates an effective and efficient internal control system?

- A. HR
- B. Senior management
- C. Line management
- D. Internal audit

Answer: B ([メッセージを残す](#))

The best answer is B. Senior management.

The culture that supports an effective internal control system is set from the top. ISACA's governance and culture guidance consistently treats culture as a management and leadership responsibility. Senior leadership establishes tone, values, expectations, accountability, and behavioral norms that shape how controls are designed, followed, and enforced across the enterprise. A strong control culture depends on visible commitment from leadership, not just procedural ownership by operational teams.

Option A. HR supports the culture through hiring, training, and policy reinforcement, but HR does not have primary accountability for the overall control environment.

Option C. Line management plays an important role in day-to-day control execution, but enterprise culture is primarily driven by senior leadership.

Option D. Internal audit evaluates and provides assurance over the control system; it does not own or establish the control culture because doing so would impair independence.

Therefore, B is the correct answer because senior management is primarily accountable for establishing the tone and culture that enable an effective and efficient internal control system.

References (Official ISACA):

- * ISACA Journal, Auditing Your Organizational Culture.
- * ISACA Now Blog, Culture as a Corporate Asset.
- * ISACA Digital Video/Podcast, Understanding and Assessing Organization Culture.
- * ISACA Journal, Auditing Culture.

最新問題: 489

Which of the following is PRIMARILY used in blockchain technology to create a distributed immutable ledger?

- A. Edge computing
- B. Encryption
- C. Application hardening
- D. Artificial intelligence (AI)

Answer: [\(解答を表示する\)](#)

Blockchain technology uses cryptographic techniques, including encryption, to secure data, verify transactions, and ensure immutability of the ledger. Cryptographic hashing, digital signatures, and encryption ensure that once data is recorded in the blockchain, it cannot be altered or tampered with, providing a secure, distributed, and immutable record.

While edge computing, application hardening, and artificial intelligence (AI) may be relevant in other contexts, encryption is central to blockchain's security and immutability features.

最新問題: 490

The use of which of the following is an inherent risk in the application container infrastructure?

- A. Shared registries
- B. Shared data
- C. Host operating system
- D. Shared kernel

Answer: [C \(メッセージを残す\)](#)

最新問題: 491

データ保持ポリシーを導入する最も適切な理由は次のうちどれですか？

- A. 災害復旧手順における復旧目標時点 (RPO)を設定する
- B. 情報の保管および保護に関連する責任を制限するため
- C. 組織内でのデータ処理に関する業務目標を文書化する
- D. データ保護に関する責任と所有権をIT部門外に委任する。

Answer: [B \(メッセージを残す\)](#)

データ保持ポリシーを導入する最大の理由は、情報の保管と保護に伴う法的責任を制限することです。データ保持ポリシーとは、企業が情報を維持するための確立された手順であり、通常、保持する必要のあるデータ、保管すべき形式、保管期間、最終的にアーカイブまたは削除するかどうか、廃棄権限を持つ者、およびポリシー違反が発生した場合の手順を定義します¹。データ保持ポリシーは、組織に次のようなメリットをもたらします。

* 財務記録、医療記録、個人データなど、特定の種類のデータの保持および廃棄を義務付ける法的および規制上の要件を遵守する

* 保存するデータ量を最小限に抑え、適切なセキュリティ対策を講じることで、データ漏洩、盗難、紛失、破損のリスクを軽減します。

ストレージスペースの利用を最適化し、バックアップおよびリカバリ操作の必要性を減らすことで、コストとリソースを節約します。

不要なデータや古いデータを排除し、データ品質とアクセス性を向上させることで、業務効率とパフォーマンスを向上させます。

* 緊急事態発生時に重要なデータが利用可能で復旧可能であることを保証することにより、事業継続計画および災害復旧計画を支援する。

* データの真正性、完全性、および出所の証拠を提供することで、監査証拠と調査を容易にします。したがって、データ保持ポリシーを導入することで、組織は情報の保存と保護に関連する責任を制限し、データガバナンスと管理の実践を改善することができます。

参考文献：

* データ保持ポリシー入門 :ベストプラクティス、事例など

最新問題: 492

コンプライアンス監査の計画段階で、情報システム監査担当者は、銀行のコンプライアンス要件一覧に、データリスク管理に関する最近の規制変更が含まれていないことを発見しました。監査担当者はまず何をすべきでしょうか？

- A. 規制変更がなぜ含まれていないのか、経営陣に問い合わせてください。
- B. 法務部と潜在的な規制上の問題について話し合う
- C. 不足している規制更新を最高情報責任者（CIO）に報告する。
- D. 最近の規制変更を監査範囲から除外する。

Answer: ([解答を表示する](#))

説明

IS監査人がコンプライアンス監査の計画段階で最初に行うべきことは、規制変更がなぜ反映されていないのかを経営陣に尋ねることです。IS監査人は、データリスク管理に関連する最近の規制変更をコンプライアンス要件のインベントリに反映させていない理由について問い合わせる必要があります。これにより、IS監査人は組織内でコンプライアンス義務の認識、伝達、または実施にギャップがあるかどうかを把握することができます。その他の選択肢は、IS監査人が最初に行うべきことではなく、経営陣の対応次第で後続的に行うべき行動です。参考文献：

CISAレビューマニュアル（デジタル版）、第2章、セクション2.31

CISA復習問題、解答、解説データベース、問題ID 214

最新問題: 493

In what way is a common gateway interface (CGI) MOST often used on a webserver?

- A. Consistent way for transferring data to the application program and back to the user
- B. Computer graphics imaging method for movies and TV
- C. Graphic user interface for web design
- D. interface to access the private gateway domain

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word or entering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

最新問題: 494

Which of the following is an advantage of prototyping?

- A. The finished system normally has strong internal controls.
- B. it ensures that functions or extras are not added to the intended system.
- C. Prototype systems can provide significant time and cost savings.
- D. Change control is often less complicated with prototype systems.

Answer: ([解答を表示する](#))

最新問題: 495

Which of the following is the MOST effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented?

- A. Ensure sufficient audit resources are allocated,
- B. Communicate audit results organization-wide.
- C. Ensure ownership is assigned.
- D. Test corrective actions upon completion.

Answer: ([解答を表示する](#))

The most effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented is to ensure ownership is assigned. This means that the management of the audited area should accept responsibility for implementing the action plans and report on their progress and completion to the audit committee or senior management. This will ensure accountability, commitment, and follow-up for the audit recommendations³⁴. References: 3: CISA ReviewManual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.6: Reporting, page 41 4: CISA Online Review Course, Module 1:

The Process of Auditing Information Systems, Lesson 1.6: Reporting

最新問題: 496

内部ネットワーク上に不正な無線アクセスポイントが存在することを検出するのに、次のうちどれが最も効果的でしょうか？

- A. 継続的なネットワーク監視
- B. 定期的なネットワーク脆弱性評価
- C. 電子アクセスログのレビュー
- D. 物理セキュリティレビュー

Answer: A ([メッセージを残す](#))

内部ネットワーク上の不正な無線アクセスポイントを検出する最も効果的な方法は、A. 継続的なネットワーク監視です。継続的なネットワーク監視では、ネットワーク内のすべての無線トラフィックをキャプチャして分析し、許可なくネットワークに接続されている可能性のある不正なデバイスやなりすましデバイスを特定できます。また、継続的なネットワーク監視は、ネットワーク上の疑わしいアクティビティや異常なアクティビティをシステム管理者に警告し、不正な無線アクセスポイントを迅速に特定して削除するのに役立ちます。

定期的なネットワーク脆弱性評価 (B) は、不正な無線アクセスポイントの検出にも役立ちますが、一定の間隔で実施されるため、評価の間に追加または削除されたデバイスを見逃す可能性があり、継続的なネットワーク監視ほど効果的ではありません。電子アクセスログのレビューは、ネットワークにアクセスするデバイスに関する情報を提供できますが、偽造または盗難された認証情報を使用するデバイスや、ログを生成しないデバイスを検出できない場合があります。物理セキュリティレビュー (D) は、ネッ

トワークポートまたはデバイスへの不正な物理的アクセスを防止するのに役立ちますが、隠蔽または正規のデバイスに偽装された無線アクセスポイントを検出できない場合があります。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 497

ミッションクリティカルなサーバーに影響を与える可能性のある新たな脆弱性に対処するための、検証済みのパッチがリリースされました。

すぐに何をすべきか？

- A. 緩和策を追加する。
- B. サーバーのセキュリティを確認し、パッチをインストールします。
- C. 影響分析を実施する。
- D. サーバーをオフラインにしてパッチをインストールします。

Answer: ([解答を表示する](#))

セクション: 情報システムの運用、保守およびサポート

最新問題: 498

ベンダーが重要な業務アプリケーションへの特権アクセスを必要としています。データ漏洩のリスクを軽減するための最適な推奨事項は次のうちどれですか？

- A. 特権ロールのリアルタイム活動監視を実装する
- B. ベンダー契約に監査権を盛り込む
- C. 特権的な役割と責任の見直しを実施する
- D. ベンダーに対し、特権ロールのジョブローテーションを実施するよう要求する。

Answer: ([解答を表示する](#))

ベンダーは、重要な業務アプリケーションへの特権アクセスを必要とします。データ漏洩のリスクを軽減するための最善策は、特権ロールに対してリアルタイムのアクティビティ監視を実施することです。リアルタイムのアクティビティ監視は、特権アクセスを持つベンダーが行うデータの作成、変更、削除、コピーなどの操作を可視化し、説明責任を確保できるためです。また、リアルタイムのアクティビティ監視は、データ漏洩を示唆する可能性のある不正または疑わしいアクティビティをタイムリーに検知し、対応することを可能にします。ベンダー契約に監査権を含めることは良い慣行ですが、監査は通常、定期的に、または必要に応じて実施されるため、データ漏洩をタイムリーに防止または検知するには十分ではない可能性があります。

特権ロールと責任のレビューを実施することも良い方法ですが、特権アクセスを持つベンダーによるデータ漏洩の具体的なリスクには対処できない可能性があります。ベンダーに特権ロールのジョブローテーションの実施を要求することで、共謀や不正行為のリスクを軽減できる可能性があります。特権アクセスを持つ個人によるデータ漏洩を防止または検出できるとは限りません。参照: CISA レビュー マニュアル (デジタル版)

[ISACA プライバシー原則およびプログラム管理ガイド]

最新問題: 499

被監査機関は、報告すべき問題点が特定された後、直ちに是正措置を講じた。

監査人は以下のことを行うべきである。

- A. IS監査人はすべての発見事項を正確に報告する責任があるため、最終報告書に発見事項を含めてください。
- B. 監査報告書には未解決の指摘事項のみを含めるべきであるため、この指摘事項は最終報告書に含めない。
- C. 監査中にIS監査人が是正措置を確認できるため、最終報告書にはこの所見を含めない。
- D. 調査結果を最終会議での議論のみに含めます。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

監査結果を最終報告書に含めることは、一般的に認められている監査実務です。監査開始後、終了前に何らかの措置が講じられた場合、監査報告書にはその所見を明記し、講じられた是正措置を記述する必要があります。監査報告書は、監査開始時点の状況を反映したものであるべきです。被監査者が講じたすべての是正措置は、書面で報告する必要があります。

最新問題: 500

IS監査担当者が、知的財産および特許を担当する部門との連携に関連するセキュリティ管理策をレビューしています。監査担当者が最も懸念すべき点は次のうちどれでしょうか？

- A. このコラボレーションツールはホストされており、インターネットブラウザ経由でのみアクセスできます。
- B. 知的財産権および特許を扱う部署に対して研修が実施されなかった
- C. 従業員はコラボレーションツールを通じて社外のユーザーとファイルを共有できます。
- D. コンテンツフィルタリングのログ記録と監視は有効になっていません。

Answer: C ([メッセージを残す](#))

最新問題: 501

What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

- A. Software escrow was not negotiated.
- B. Several vendor deliverables missed the commitment date.
- C. An operational level agreement (OLA) was not negotiated.
- D. The contract does not contain a right-to-audit clause.

Answer: A ([メッセージを残す](#))

最新問題: 502

ある組織が最近クラウド文書ストレージソリューションを導入し、エンドユーザーがローカルワークステーションのハードドライブにデータを保存する機能を削除しました。IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？

- A. ユーザーは更新された利用規約に署名する必要はありません。
- B. ユーザーは新しいシステムに関するトレーニングを受けていません。
- C. 事業継続計画 (BCP) が更新されていませんでした。
- D. モバイル端末は暗号化されていません。

Answer: (解答を表示する)

これはIS監査担当者にとって最大の懸念事項となるはずです。なぜなら、組織がクラウド文書ストレージソリューションが、業務の中断や災害発生時に事業継続能力に及ぼす潜在的な影響を考慮していないことを意味するからです。BCP（事業継続計画は、危機発生時および発生後に重要な事業機能を維持または再開するために講じるべき手順と措置を概説した文書です。BCPは、クラウド文書ストレージソリューションの導入など、組織のITインフラストラクチャ、システム、プロセス、または依存関係に大きな変更があった場合は、必ず更新する必要があります。IS監査担当者は、BCPが組織のIT環境の現状を反映していること、およびクラウド文書ストレージソリューションに関連するリスク、課題、機会に対処していることを検証する必要があります。

他の選択肢は、BCPが更新されていないことほど懸念すべきものではありません。

* 利用者は、更新された利用規約に署名する必要はありません。これは些細な懸念事項ではありますが、組織の事業継続性にとって重大な脅威となるものではありません。利用規約とは、クラウド文書ストレージソリューションなどのITリソースの使用に関する規則とガイドラインを定めた文書です。利用者は、自身の責任と義務を認識し、組織のポリシーと基準を遵守するために、更新された利用規約に署名する必要があります。しかし、これは危機発生時に組織が事業を継続する能力に影響を与えるものではありません。

* ユーザーは新システムに関するトレーニングを受けていません。これは中程度の懸念事項ではありますが、組織の事業継続性を脅かすものではありません。ユーザーが新システムを効果的かつ効率的に使用できるように、またシステムのセキュリティやパフォーマンスを損なう可能性のあるエラーや誤用を回避するためには、新システムに関するトレーニングが重要です。ただし、これは組織が危機時にデータにアクセスしたり、データを復元したりすることを妨げるものではありません。

* モバイルデバイスは暗号化されていません。これは重大な懸念事項ですが、組織の事業継続性に直接的な影響を与えるものではありません。モバイルデバイスの暗号化は、紛失や盗難の際に、デバイスに保存されているデータを不正アクセスや漏洩から保護するセキュリティ対策です。しかし、これはクラウド文書ストレージソリューションに保存されているデータの可用性や完全性には影響しません。クラウド文書ストレージソリューションには独自の暗号化メカニズムが備わっているはずです。

最新問題: 503

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- A. meets or exceeds industry security standards.
- B. agrees to be subject to external security reviews.
- C. has a good market reputation for service and experience.
- D. complies with security policies of the organization.

Answer: B (メッセージを残す)

Section: Protection of Information Assets

Explanation:

It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify or prove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

最新問題: 504

パスワード漏洩に伴うリスクを最も効果的に軽減できる対策はどれですか？

- A. パスワードには形式制限があります。
- B. パスワードはクラウドに保存されます。
- C. パスワードはアプリケーションごとに固有です。
- D. パスワードはマスクされています。

Answer: ([解答を表示する](#))

最新問題: 505

IT統制目標は、IS監査人にとって有用であり、以下の点を理解するための基礎となる。

- A. 特定の管理手順を実施する際の望ましい結果または目的。
- B. 特定の組織に関連する最良のITセキュリティ管理手法。
- C. 情報セキュリティのための技術。
- D. セキュリティポリシー。

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

IT統制目標とは、特定のIT活動において統制手順を実施することによって達成されるべき望ましい結果または目的を記述したものです。これらは統制を実施するための具体的な目標を示し、必ずしもベストプラクティスであるとは限りません。手法とは目標を達成するための手段であり、セキュリティポリシーはIT統制目標の一部です。

最新問題: 506

アプリケーションシステムの監査について語る際には、常に以下の点に重点を置くべきです。

- A. システムの性能と制御
- B. 不正アクセスや不正操作を制限する機能
- C. 入力されたデータは正しく処理されました
- D. データ出力は正しく処理されています
- E. システムへの変更は適切に承認されています
- F. 選択肢に該当しない。

Answer: A,B,C,D,E ([メッセージを残す](#))

アプリケーションシステムの監査について言えば、システムのパフォーマンスと制御、不正アクセスや改ざんを制限する能力、システム上でのデータ入出力が正しく処理されていること、システムへの変更がすべて承認されていること、そしてユーザーがシステムにアクセスできることに重点を置くべきです。

最新問題: 507

以下の物理的アクセス制御のうち、データセンターへの不正アクセスを最も効果的に防止できるのはどれですか？

- A. 暗号錠
- B. 手のひら読み取りとPINコード
- C. スマートカードと物理キー
- D. バッジアクセス

Answer: B ([メッセージを残す](#))

最新問題: 508

A review of IT interface controls finds an organization does not have a process to identify and correct records that do not get transferred to the receiving system.

Which of the following is the IS auditor's BEST recommendation?

- A.** Implement software to perform automatic reconciliations of data between systems.
- B.** Have coders perform manual reconciliation of data between systems.
- C.** Enable automatic encryption, decryption, and electronic signing of data files.
- D.** Automate the transfer of data between systems as much as feasible.

Answer: A ([メッセージを残す](#))

最新問題: 509

Which of the following technique is used for speeding up network traffic flow and making it easier to manage?

- A.** Point-to-point protocol
- B.** X.25
- C.** MPLS
- D.** ISDN

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

For your exam you should know below information about WAN Technologies:

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Point-to-point protocol

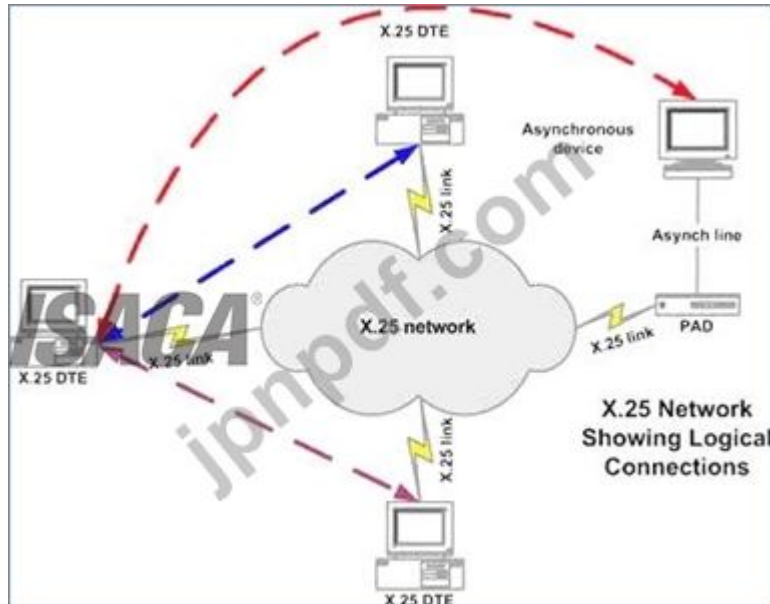
X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.



X.25

Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality.

Frame relay is any to any service.

Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.

ISDN

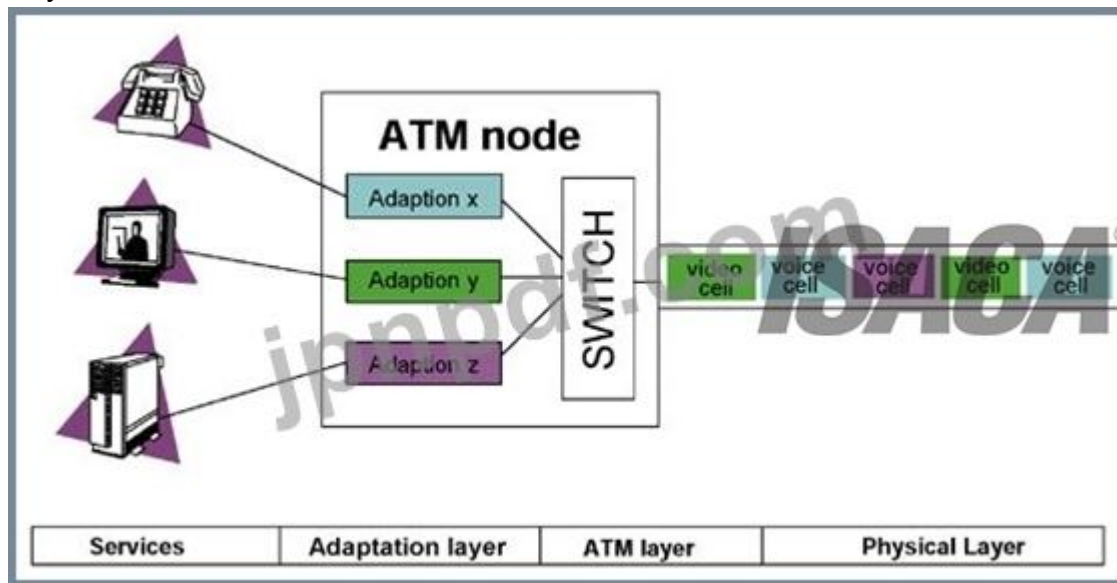
Asynchronous Transfer Mode (ATM)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes Some companies have replaces FDDI back-end with ATM

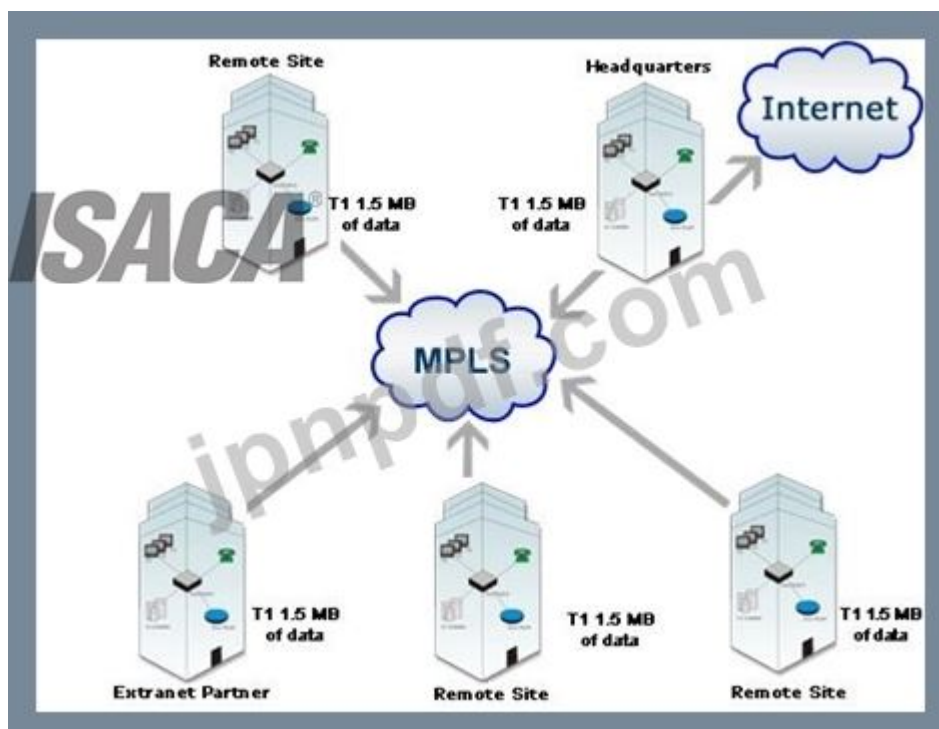
Asynchronous Transfer Mode



Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

X.25 - X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication. X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Point-to-point protocol - PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.

ISDN - Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

最新問題: 510

IS監査担当者が、退職した従業員のアクセス権を削除するプロセスが文書化されていないことを発見しました。この発見から最も重大なリスクは何ですか？

- A. 手順がベストプラクティスと一致しない可能性があります
- B. 人事 (HR) 記録がシステムアクセスと一致しない場合があります。
- C. 不正アクセスは特定できません。
- D. アクセス権限が適時に削除されない場合があります。

Answer: ([解答を表示する](#))

この観察結果から最も重大なリスクは、アクセス権限が適時に削除されない可能性があることです。退職した従業員のアクセス権限を削除するプロセスが文書化されていない場合、誰が、どのように、いつ、どのような措置を講じて組織を離れる従業員のアクセス権限を取り消すべきかについて、明確な指針や責任の所在が示されません。これにより、アクセス権限の削除に遅延、矛盾、または漏れが生じ、退職した従業員が組織のシステムやデータへの不正アクセスを保持してしまう可能性があります。これは、情報資産のセキュリティ、機密性、完全性、および可用性を損なう可能性があります。参考文献：

* CISAレビューマニュアル (デジタル版)

* CISAに関する質問、回答、解説データベース

最新問題: 511

Which of the following would provide management with the MOST reasonable assurance that a new data warehouse will meet the needs of the organization?

- A. Integrating data requirements into the system development life cycle (SDLC)
- B. Appointing data stewards to provide effective data governance
- C. Classifying data quality issues by the severity of their impact to the organization
- D. Facilitating effective communication between management and developers

Answer: A ([メッセージを残す](#))

Explanation

A data warehouse is a centralized repository of data that is collected from various sources and organized for analysis and reporting purposes. A data warehouse can help an organization gain insights into its business performance, trends, and opportunities. However, building a data warehouse requires careful planning, design, and implementation to ensure that it meets the needs of the organization.

One of the best practices that would provide management with the most reasonable assurance that a new data warehouse will meet the needs of the organization is A. Integrating data requirements into the system development life cycle (SDLC). The SDLC is a framework that defines the phases and activities involved in developing a software system, such as planning, analysis, design, testing, deployment, and maintenance¹. By integrating data requirements into the SDLC, an organization can ensure that the data warehouse is aligned with the business objectives and expectations, and that it delivers value to the end users.

Some of the benefits of integrating data requirements into the SDLC are:

It helps to identify and prioritize the key business questions and metrics that the data warehouse should support².

It helps to define and validate the data sources, models, structures, and quality standards that the data warehouse should follow³.

It helps to design and implement the data integration, transformation, and loading processes that the data warehouse should use⁴.

It helps to test and verify the functionality, performance, and accuracy of the data warehouse before deploying it to production.

It helps to monitor and maintain the data warehouse after deployment and incorporate feedback and changes as needed.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 512

Which of the following is the BEST way to mitigate the impact of ransomware attacks?

- A. Invoking the disaster recovery plan (DRP)
- B. Backing up data frequently
- C. Paying the ransom
- D. Requiring password changes for administrative accounts

Answer: B (メッセージを残す)

Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom for its decryption¹.

Ransomware attacks can cause significant damage to an organization's operations, reputation, and finances¹. Therefore, it is important to mitigate the impact of ransomware attacks by implementing effective prevention and recovery strategies.

One of the best ways to mitigate the impact of ransomware attacks is to back up data frequently¹²³⁴⁵. Data backups are copies of the organization's data that are stored in a separate location or medium, such as an external hard drive, cloud storage, or tape². Data backups can help the organization restore its data in case of a ransomware attack, without paying the ransom or losing valuable information². Data backups should be performed regularly, preferably daily or weekly, depending on the criticality and volume of the data². Data backups should also be tested periodically to ensure their integrity and usability².

The other options are not as effective as backing up data frequently in mitigating the impact of ransomware attacks. Invoking the disaster recovery plan (DRP) is a reactive measure that can help the organization resume its operations after a ransomware attack, but it does not prevent or reduce the damage caused by the attack³.

Paying the ransom is not a recommended option, as it does not guarantee the decryption of the data or the deletion of the stolen data by the attackers. Paying the ransom also encourages further attacks and funds criminal activities¹⁴. Requiring password

changes for administrative accounts is a good security practice, but it is not sufficient to prevent or recover from ransomware attacks. Ransomware attacks can exploit other vulnerabilities, such as phishing emails, outdated software, or weak network security¹⁵.

References: 1: How to Mitigate the Risk of Ransomware Attacks: The Definitive Guide 2: Mitigating malware and ransomware attacks - The National Cyber Security Centre 3: 3 steps to prevent and recover from ransomware 4: Ransomware Epidemic: Use these 8 Strategies to Mitigate Risk 5: Practical Steps to Mitigate Ransomware Attacks - ITSecurityWire

最新問題: 513

情報セキュリティプログラムの成功にとって、次のうちどれが最も重要ですか？

- A. 情報セキュリティとIT目標の整合性
- B. 経営陣の情報セキュリティへの取り組み
- C. ビジネスと情報セキュリティの統合
- D. 情報セキュリティに対するユーザーの責任

Answer: B ([メッセージを残す](#))

説明

正解はBです。経営陣の情報セキュリティへの取り組み。経営陣の情報セキュリティへの取り組みは、情報セキュリティプログラムの成功にとって最も重要な要素です。なぜなら、経営陣は安全な環境を確立し維持するために必要なリーダーシップ、サポート、リソースを提供するからです。

経営陣の情報セキュリティへの取り組みは、以下の点によって示すことができる。

情報セキュリティのビジョン、ミッション、目標を設定し、それらを組織の戦略と目標に整合させる1。

情報セキュリティに関する方針、基準、手順を確立し、施行し、関連する法律および規制の遵守を確保する1。

情報セキュリティのために十分な予算、人員、技術を割り当て、トレーニングと啓発プログラムに投資する2。

組織内でセキュリティ文化を促進し、ステークホルダーやパートナーと連携して信頼と協力を育む2。

最新問題: 514

Which of the following poses the GREATEST security risk when implementing acquired application systems?

- A. Password length
- B. Social engineering
- C. Default logon IDs
- D. Lack of audit logs

Answer: C ([メッセージを残す](#))

最新問題: 515

IT災害復旧目標時間 (RTO)は、以下の点に基づいて設定する必要があります。

- A. システム間の相互依存関係。
- B. 許容される最大データ損失。
- C. 最大許容ダウンタイム (MTD)。
- D. 平均復旧時間 (MTTR)。

Answer: C ([メッセージを残す](#))

最新問題: 516

トップダウン型の成熟度モデルプロセスを採用した場合、次のうちどれが結果として生じるでしょうか？

- A. 企業内の他のプロセスの有効性を比較する手段
- B. 最も改善の余地があるプロセスの特定
- C. 同業他社との類似プロセスの有効性をベンチマークする手段
- D. タイムリーな見直しを確実にするため、より古く確立されたプロセスを特定する。

Answer: B ([メッセージを残す](#))

最新問題: 517

IS監査担当者が、ユーザーが特定の映画を視聴する可能性を予測する機械学習（ML）モデルをレビューしています。監査担当者にとって最も懸念されるのは次のうちどれでしょうか？

- A. モデルの開発にはオープンソースのプログラミング言語が使用されました。
- B. このモデルは、トレーニングデータと同じ母集団から抽出されたデータでテストされました。
- C. 異なる母集団から得られたデータでモデルをテストしたところ、精度が低下しました。
- D. モデルのトレーニングに使用したデータセットは信頼性の低い情報源から入手したものです。

Answer: ([解答を表示する](#)**)**

正解はDです。モデルの学習に使用したデータセットは、信頼性の低い情報源から入手したものです。

ISACAのAIおよび機械学習に関するガイダンスでは、入力データとトレーニングデータの品質、信頼性、および検証が非常に重要視されています。ISACAは、各データソースを検証する管理体制が必要であり、破損した、または品質の低いトレーニングデータは、結果の品質低下につながる可能性がある」と指摘しています。トレーニングデータセットが信頼性の低いソースから取得された場合、モデルの予測は、最初から根本的に欠陥があったり、偏っていたり、操作されていたり、監査不可能であったりする可能性があります。

選択肢A :オープンソースのプログラミング言語は、本質的に懸念事項ではありません。言語自体が、モデルの信頼性や制御性を決定づけるものではありません。

オプションB :トレーニングデータと同じ母集団のデータでテストすることは、一般的な検証手順であり、それ自体は本質的に問題ではありません。

選択肢C. 異なる集団で精度が低下することは、一般化可能性に関する懸念事項となり得るが、この問題においては、信頼性の低い訓練データの方がより根本的な問題である。ソースデータ自体が信頼できない場合、その後のすべての結果が疑わしいものとなる。

したがって、Dが正解です。なぜなら、信頼性の低い訓練データは、モデルの妥当性と信頼性に対する最も深刻な基礎的リスクを生み出すからです。

参考文献（ISACA公式）：

* ISACAジャーナル、信頼できるAIの開発：入力理解」。

* ISACAジャーナル、人工知能が監査に与える影響—新興技術」。

* ISACAのプレスリリース ISACAの新しい出版物では、機械学習技術と監査人向けのコンプライアンスリスクに焦点を当てています。」

* ISACA、AIアルゴリズム監査：主要な統制上の考慮事項。

最新問題: 518

次のうち、ipfwadm の書き換え版はどれですか？

- A. ipchains
- B. iptables
- C. ネットフィルター
- D. ipcook
- E. 選択肢のどれもでない。

Answer: A ([メッセージを残す](#))

ipchainsは、以前のLinux上で動作するフリーソフトウェアベースのファイアウォールです。ipfwadmのリライト版ですが、Linux 2.4以降ではiptablesに置き換えられています。iptablesは、Linuxカーネル内のパケットフィルタリングとNATコンポーネントを制御します。これは、ネットワークパケットの傍受と操作のためにLinuxカーネル内に一連のフックを提供するフレームワークであるNetfilterに基づいています。

最新問題: 519

災害復旧テスト中に、IS監査担当者は災害復旧サイトのサーバーのパフォーマンスが遅いことに気づきました。この根本原因を特定するために、IS監査担当者はまず以下を確認する必要があります。

- A. 災害復旧サイトで生成されたイベントエラーログ。
- B. 災害復旧テスト計画。
- C. 災害復旧計画 (DRP)。
- D. プライマリサイトと災害復旧サイトの構成と配置。

Answer: D ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

システム構成が最も可能性の高い原因であるため、IS監査担当者はまずその構成を確認する必要があります。問題が解決しない場合は、IS監査担当者はイベントエラーログを確認する必要があります。災害復旧テスト計画および災害復旧計画 (DRP) には、システム構成に関する情報は含まれていません。

最新問題: 520

.When should application controls be considered within the system-development process?

- A. After application unit testing
- B. After application module testing
- C. After applications systems testing
- D. As early as possible, even in the development of the project's functional specifications

Answer: D ([メッセージを残す](#))

Application controls should be considered as early as possible in the system-development process, even in the development of the project's functional specifications.

最新問題: 521

Which of the following refers to the proving of mathematical theorems by a computer program?

- A. Analytical theorem proving
- B. Automated technology proving

- C. Automated theorem processing
- D. Automated theorem proving
- E. None of the choices.

Answer: D ([メッセージを残す](#))

Automated theorem proving (ATP) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification.

最新問題: 522

Which of the following is MOST important to ensure when developing an effective security awareness program?

- A. Training personnel are information security professionals.
- B. Outcome metrics for the program are established.
- C. Security threat scenarios are included in the program content.
- D. Phishing exercises are conducted post-training

Answer: B ([メッセージを残す](#))

Explanation

The most important factor to ensure when developing an effective security awareness program is B. Outcome metrics for the program are established. This is because outcome metrics are measures that evaluate the impact and results of the security awareness program on the behavior and performance of the users, and the security posture and objectives of the organization¹.

Outcome metrics can help ensure the effectiveness of the security awareness program by:

Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate¹.

Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency¹.

Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program¹.

最新問題: 523

アジャイル開発手法に基づいたシステムソフトウェア開発プロジェクトをレビューするIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？

- A. 変更管理に関する文書の不足
- B. ユーザー受け入れテスト (UAT)の承認不足
- C. 安全なコーディング手法の欠如
- D. 毎週の制作リリースがない

Answer: ([解答を表示する](#))

最新問題: 524

セキュリティ分類の異なるデータを含むサーバー上で、最小権限の原則を徹底するための最適な方法は次のうちどれですか？

- A. データ所有者が決定したアクセス制御を適用する
- B. ユーザーからデータ分類ポリシーへの準拠に関する正式な同意を得る

- C. スクリプト化されたアクセス制御リストを使用して、サーバーへの不正アクセスを防止する
- D. 使用頻度に基づいてデータファイルへのアクセスを制限する

Answer: A ([メッセージを残す](#))

最新問題: 525

コントロール自己評価 (CSA)は、以下の目的で使用できます。

- A. 資産の価値を決定する。
- B. 基準値を設定する。
- C. 戦略的な事業目標を評価する。
- D. 監査を置き換える。

Answer: B ([メッセージを残す](#))

内部統制自己評価 (CSA)は、事業部門が内部統制の有効性を評価できるプロセスです。主に、統制の有効性とリスク管理を測定するための基準値 (オプションB)を設定するために使用されます。

ISACA CISA参照 :CSAは、リスク評価と統制改善を支援する、認知された内部統制メカニズムです。

リスクへの影響 :CSAが適切に実施されない場合、組織は脆弱な統制を把握できず、リスクにさらされる可能性が高まる。

代替案 :

選択肢A :CSAは資産評価に重点を置いていません。

選択肢C : 戦略的な事業目標は、ガバナンスプロセスを通じて個別に評価される。

選択肢D :CSAは正式な監査を補完するものであり、代替するものではありません。

最新問題: 526

The BEST filter rule for protecting a network from being used as an amplifier in a denial of service (DoS) attack is to deny all:

- A. outgoing traffic with IP source addresses external to the network.
- B. incoming traffic with discernible spoofed IP source addresses.
- C. incoming traffic with IP options set.
- D. incoming traffic to critical hosts.

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Outgoing traffic with an IP source address different than the IP range in the network is invalid, in most of the cases, it signals a DoS attack originated by an internal user or by a previously compromised internal machine; in both cases, applying this filter will stop the attack.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 527

IS監査担当者は、システム障害のビジネスへの影響を最も適切に評価するために、以下の方法を用いることができます。

- A. 機器保守ログの分析。
- B. ユーザー満足度レベルの評価。
- C. システム生成ログの確認。
- D. セキュリティ管理者へのインタビュー。

Answer: B ([メッセージを残す](#))

最新問題: 528

When evaluating a protect immediately prior to implementation, which of the following would provide the BEST evidence that the system has the required functionality?

- A. Quality assurance (QA) results
- B. Sign-off from senior management
- C. User acceptance testing (UAT) results
- D. Integration testing results

Answer: A ([メッセージを残す](#))

最新問題: 529

電子メールシステムが訴訟における有用な証拠源となった最も可能性の高い理由は、次のうちどれでしょうか？

- A. 複数のバックアップファイルが利用可能です。
- B. アクセス制御は、電子メール活動に対する責任を確立します。
- C. データ分類は、電子メールで伝達すべき情報を規定します。
- D. 企業内では、電子メールの使用に関する明確なポリシーにより、証拠が確実に利用可能になります。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

削除されたはずの文書を含むバックアップファイルは、これらのファイルから復元される可能性があります。アクセス制御は特定の文書の発行責任を確立するのに役立つかもしれませんが、電子メールの証拠にはなりません。電子メールで伝達すべき内容に関するデータ分類基準が定められている場合もありますが、その方針を策定しただけでは、訴訟に必要な情報は得られません。

最新問題: 530

Which of the following is BEST used for detailed testing of a business application's data and configuration files?

- A. Version control software
- B. Audit hooks
- C. Utility software
- D. Audit analytics tool

Answer: D ([メッセージを残す](#))

The best tool for detailed testing of a business application's data and configuration files is an audit analytics tool. An audit analytics tool is a software that helps auditors to analyze large sets of data and identify anomalies, trends, and patterns that are

relevant to the audit objectives. An audit analytics tool can also provide audit evidence and support the auditor's professional judgment and conclusions.

Some of the benefits of using an audit analytics tool are:

It can improve the efficiency and effectiveness of the audit by reducing the time and effort required to perform manual tests and procedures.

It can enhance the quality and reliability of the audit by increasing the coverage and accuracy of the data analysis and testing.

It can enable the auditor to perform more complex and sophisticated tests and procedures that may not be possible or feasible with traditional methods.

It can help the auditor to discover new insights and risks that may not be apparent or detectable with traditional methods.

Some examples of audit analytics tools are:

IDEA: A data analysis software that allows auditors to import, analyze, and visualize data from various sources and formats. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, and regression analysis.¹

ACL: A data analysis software that helps auditors to access, analyze, and report on data from various sources and formats. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, regression analysis, and scripting.²

TeamMate Analytics: A data analysis software that integrates with Microsoft Excel and provides auditors with a range of tools and functions to perform data analysis and testing. It also offers features such as sampling, stratification, gap analysis, duplicate detection, Benford's law, regression analysis, and scripting.³

最新問題: 531

既存のIT能力をベンチマークする際に、以下のツールのうちどれが最も役立ちますか？

- A. 過去のIS監査報告書
- B. IT成熟度モデル
- C. リスク評価
- D. ITバランススコアカード

Answer: D ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 532

An IS auditor is asked to provide feedback on the systems options analysis for a new project. The BEST course of action for the IS auditor would be to:

- A. identify the best alternative.
- B. request at least one other alternative.
- C. comment on the criteria used to assess the alternatives.
- D. retain comments as findings for the audit report.

Answer: ([解答を表示する](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 533

プロジェクト運営委員会の主な責任は以下のとおりです。

- A. 最終ビルドドキュメントに署名する。

- B. 各プロジェクトの納期を確実に守る。
- C. 開発されたシステムがビジネスニーズを満たしていることを確認する。
- D. 定期的なプロジェクト進捗状況の報告と監督を行う。

Answer: D ([メッセージを残す](#))

プロジェクト運営委員会の主な責務は、プロジェクトの進捗状況を定期的に報告し、監督を行うことである。

プロジェクト運営委員会は、上級関係者や専門家で構成される諮問グループであり、プロジェクトマネージャーとそのチームに指導と支援を提供します。運営委員会は主に、特定のプロジェクトを実現するための方向性、範囲、予算、スケジュール、および方法に関与します。

運営委員会の重要な役割の一つは、プロジェクトの進捗状況とパフォーマンスを監視し、それがビジネス目標と利害関係者の期待に合致していることを確認することです。運営委員会はまた、プロジェクトマネージャーにフィードバック、アドバイス、推奨事項を提供し、プロジェクトライフサイクル中に発生する可能性のある問題や課題の解決を支援します。運営委員会は、会議、レポート、プレゼンテーションなどを通じて、プロジェクトマネージャーや他の利害関係者と定期的にコミュニケーションを取ります²³。

したがって、定期的なプロジェクト状況の報告と監督は、プロジェクト運営委員会の主要な責任である。

参考文献：

運営委員会：定義 役割、会議のヒント - ProjectManager プロジェクト運営委員会：役割 ベストプラクティス、課題 - ProjectPractical 運営委員会：例とテンプレートを含む完全ガイド - Status.net

最新問題: 534

When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

- A. The business case.
- B. The project schedule.
- C. Proposed enhancements.
- D. Quality assurance (QA) results.

Answer: A ([メッセージを残す](#))

The business case defines the project's expected benefits, success criteria, and performance metrics. Reviewing the business case allows the auditor to assess whether the benefits identified at initiation have been realized post-implementation. The schedule (B) only tracks timeliness, not value. Proposed enhancements (C) address future improvements, not whether benefits have been delivered. QA results (D) reflect product quality but not business value. ISACA emphasizes that value delivery and benefits realization are key elements of enterprise governance of IT, aligning with COBIT's EDM02 (Ensure Benefits Delivery).

最新問題: 535

An organization considering the outsourcing of a business application should FIRST:

- A. define service level requirements.
- B. perform a vulnerability assessment.
- C. conduct a cost-benefit analysis.
- D. issue a request for proposal (RFP).

Answer: D ([メッセージを残す](#))

An RFP is a document used to solicit bids from potential vendors and to outline the requirements for a particular project. It typically includes a description of the project, a list of the requirements, and the criteria for evaluating the bids. The RFP outlines the bidding process and contract terms and establishes a strong foundation for the organization in a procurement process

最新問題: **536**

Which of the following is a passive attack on a network?

- A. Message service interruption
- B. Message modification
- C. Traffic analysis
- D. Sequence analysis

Answer: C ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: **537**

Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

- A. Application programming and systems analysis
- B. Database administration and computer operations
- C. Security administration and application programming
- D. Computer operations and application programming

Answer: ([解答を表示する](#)**)**

最新問題: **538**

内部侵入テストを計画する際、テスト範囲を確定する前に最も重要なステップは次のうちどれですか？

- A. 侵入テストの範囲をテスト環境に限定する
- B. 検査範囲について経営陣の書面による同意を得る
- C. テスト範囲についてITセキュリティ部門に通知する
- D. IT部門とテスト範囲から除外するシステムについて合意する

Answer: B ([メッセージを残す](#))

説明

テスト範囲を確定する前に、経営陣から書面でテスト範囲への同意を得ることが最も重要なステップです。これは、侵入テスト担当者がテスト活動を実行するための権限と承認を得ていることを保証するためです。また、不正アクセスや損害に関する法的責任や告発から担当者を保護することにもなります。その他の選択肢は、経営陣の同意を得ることほど重要ではなく、具体的な状況や合意内容によって異なる場合があります。例えば、一部のシステムはテスト範囲から除外できない場合があります、一部のテストはテスト環境に限定されない場合があります。参考文献 :CISAレビューマニュアル (デジタル版)1、381～382ページ。

最新問題: **539**

Disaster recovery planning (DRP) for a company's computer system usually focuses on:

- A. operations turnover procedures.
- B. strategic long-range planning.

- C. the probability that a disaster will occur.
- D. alternative procedures to process transactions.

Answer: D ([メッセージを残す](#))

It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

最新問題: 540

ある組織のセキュリティチームが、複数の脆弱性のあるアプリケーションを含む模擬的な本番環境を作成しました。このような環境を作成する主な目的は何でしょうか？

- A. サイバー攻撃のデジタル証拠を収集する
- B. 攻撃者の行動を研究するために攻撃者を誘い込む
- C. セキュリティ管理者への研修を提供する
- D. 侵入検知システム (IDS) のテスト

Answer: B ([メッセージを残す](#))

説明

複数の脆弱なアプリケーションを含む模擬的な本番環境を作成する主な目的は、攻撃者を引き付けてその行動を研究することです。これはハニーポッティングと呼ばれる手法で、攻撃者を実際のシステムを模倣した偽のシステムまたはネットワークに誘い込む欺瞞型セキュリティの一種ですが、そのシステムは隔離され監視されています¹。ハニーポッティングは、セキュリティチームが攻撃者の手法、ツール、動機、およびターゲットについて学び、組織のセキュリティ体制を改善するために使用できる貴重な情報を収集するのに役立ちます¹。ハニーポッティングは、攻撃者の注意を実際の資産からそらし、時間とリソースを浪費するのにも役立ちます²。

その他のオプションは、複数の脆弱なアプリケーションを含む模擬的な本番環境を作成する主な目的ではありません。サイバー攻撃のデジタル証拠を収集するには、セキュリティチームは、侵害されたシステムまたはネットワークからデータを保存および分析できるフォレンジックツールと技術を使用する必要があります³。セキュリティマネージャーにトレーニングを提供するには、セキュリティチームは、サイバーインシデントへの対応におけるスキルと知識をテストおよび向上できるシミュレーションツールとシナリオを使用する必要があります⁴。侵入検知システム (IDS) をテストするには、セキュリティチームは、悪意のある活動を検出および防止するIDSの有効性とパフォーマンスを評価できる侵入テストツールと方法を使用する必要があります⁵。

参考文献：

ハニーポットとは？ | Imperva

ハニーポット：侵入者を特定するための甘い解決策 | CSO Online

デジタルフォレンジック - 概要 | ScienceDirect Topics

サイバーセキュリティ訓練と演習 - 国土安全保障省

ペネトレーションテストとは？ | 種類と段階 | Imperva

最新問題: 541

IT部門の目標が組織の目標と一致しているかどうかを判断する上で、最も役立つのは次のうちどれですか？

- A. エンタープライズアーキテクチャ (EA)
- B. 主要業績評価指標 (KPI)
- C. エンタープライズダッシュボード
- D. バランススコアカード

Answer: D ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 542

When developing a risk-based IS audit plan, the PRIMARY focus should be on functions:

- A. considered important by IT management.
- B. with the most ineffective controls.
- C. with the greatest number of threats.
- D. considered critical to business operations.

Answer: D ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 543

IT management wants transferred staff to have current and previous role access to facilitate transitioning and training of new staff. Which of the following is the GREATEST risk to the organization from this practice?

- A. An increased likelihood that internal fraud will not be detected
- B. An increased impact from loss of key staff
- C. An increased number of help desk tickets due to password changes
- D. An increased number of user access recertification records

Answer: A ([メッセージを残す](#))

Allowing transferred staff to retain access from previous roles violates the principle of least privilege and increases the risk of inappropriate access. This creates a greater likelihood that internal fraud or unauthorized activities could occur without detection, as users may retain access to systems or data unrelated to their current responsibilities.

最新問題: 544

Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

- A. Direct access attacks
- B. Indirect access attacks
- C. Port attack
- D. Window attack
- E. Social attack
- F. None of the choices.

Answer: A ([メッセージを残す](#))

Direct access attacks make use of common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system

modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

最新問題: 545

A staff accountant regularly uploads spreadsheets with inventory levels to the organization's financial reporting system. The transfers are executed through a customized interface created by an in-house developer.

Which of the following is MOST important for the IS auditor to confirm during a review of the interface?

- A.** The data in the spreadsheet is correctly recorded in the financial system.
- B.** The financial system transfers are performed by the accountant at predefined intervals.
- C.** The spreadsheets do not contain malware or malicious macros.
- D.** The data transfer connection does not support full duplex communication.

Answer: ([解答を表示する](#))

Comprehensive and Detailed Explanation:

The primary audit concern is data integrity-ensuring that the data uploaded via the custom interface is accurately and completely transferred to the financial system.

- * Option A directly addresses data accuracy and integrity.
- * Option B (timing) is secondary compared to correctness.
- * Option C (malware checks) is important but handled by security controls, not the primary audit concern here.
- * Option D (duplex communication) is irrelevant to ensuring accurate financial records.

ISACA Reference: CISA Review Manual 27th Edition, Domain 3, section on interface controls and audit considerations.

最新問題: 546

When planning a follow-up, the IS auditor is informed by operational management that recent organizational changes have addressed the previously identified risk and implementing the action plan is no longer necessary.

What should the auditor do NEXT?

- A.** Report that the changes make it impractical to determine whether the risks have been addressed.
- B.** Accept management's assertion and report that the risks have been addressed.
- C.** Determine whether the changes have introduced new risks that need to be addressed.
- D.** Review the changes and determine whether the risks have been addressed.

Answer: ([解答を表示する](#))

Explanation

When operational management informs the IS auditor that recent organizational changes have addressed previously identified risks and implementing the action plan is no longer necessary, the IS auditor should accept management's assertion and report that the risks have been addressed. However, it is essential to document this communication and ensure that there is evidence supporting management's claim. If there are any doubts or concerns, further investigation may be necessary. The auditor should not assume new risks without proper assessment or evidence¹. References: 1(<https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/enhancing-the-aud>)

最新問題: 547

申請審査を計画する際に最も重要なことは、以下の項目についてインタビューを行い、リスク要因を評価することです。

- A.** プロセスオーナー

- B. アプリケーションユーザー
- C. ITマネジメント
- D. アプリケーション所有者

Answer: A ([メッセージを残す](#))

最新問題: 548

包括的な情報システム監査ポリシーには、内部監査チームがどのような役割を担うべきかを詳細に定めたガイドラインを含めるべきである。

- A. 主要なOSアプリケーションの開発とコーディング。
- B. 主要なウェブアプリケーションの取得と保守。
- C. アプリケーション開発プロジェクトの人材管理サイクルにおいて。
- D. 主要アプリケーションの開発、取得、変換、およびテストにおいて。
- E. 選択肢のどれもでない。

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

監査方針には、主要アプリケーションの開発、取得、移行、テストにおいて内部監査がどのような役割を果たすかを詳細に定めたガイドラインを含めるべきである。このような方針は、有効性を確保するために経営陣の承認を得なければならない。

最新問題: 549

Aligning IT strategy with business strategy PRIMARILY helps an organization to:

- A. optimize investments in IT.
- B. create risk awareness across business units.
- C. increase involvement of senior management in IT.
- D. monitor the effectiveness of IT.

Answer: ([解答を表示する](#)**)**

Explanation

Aligning IT strategy with business strategy primarily helps an organization to optimize investments in IT. This is because alignment ensures that IT resources and capabilities are aligned with the business goals and priorities, and that IT delivers value to the business in terms of efficiency, effectiveness, innovation, and competitive advantage¹². By aligning IT strategy with business strategy, an organization can avoid wasting money and time on IT projects or services that do not support or contribute to the business outcomes³. Alignment also helps to identify and prioritize the most critical and valuable IT initiatives that can create or optimize business value⁴.

Therefore, the correct answer to your question is A. optimize investments in IT.

最新問題: 550

コーディング標準は、次のうちどれを提供しますか？

- A. プログラムドキュメント
- B. アクセス制御テーブル
- C. データフロー図

D. フィールド命名規則

Answer: ([解答を表示する](#))

コーディング標準は、プログラム内の変数、定数、関数、クラス、その他の要素に名前を付けるための規則であるフィールド命名規則を提供します。コーディング標準は、コードの一貫性、可読性、保守性、移植性を確保するのに役立ちます。プログラムのドキュメント、アクセス制御テーブル、データフロー図は、コーディング標準の一部ではありません。参照 :CISAレビューマニュアル (デジタル版)、第4章、セクション4.3.1

最新問題: **551**

第4世代言語 (4GL)は、アプリケーションのグラフィカルユーザーインターフェース (GUI)の設計に最適です。しかし、データ計算処理を大量に行う設計には適していません。正誤を答えなさい。

A. 真

B. 偽

Answer: ([解答を表示する](#))

説明／参考資料 :

Explanation:

第4世代言語 (4GL)は、アプリケーションのグラフィカルユーザーインターフェース (GUI)の設計に最適です。しかし、データ計算を多用する複雑な処理の設計には適していません。

最新問題: **552**

IS監査担当者は、異なる送信元から受け取ったクライアントからのリクエストが複数回処理されていたことを発見した。

独立した部門別データベースは毎週同期されます。最適な方法はどれでしょうか？

おすすめ？

A. 異なる部門システム間でのデータ複製頻度を増やして、タイムリーな更新情報。

B. すべてのリクエスト処理を1つの部門に集中させ、同じリクエストの並行処理を回避します。

C. アプリケーションアーキテクチャを変更し、共通データはすべてのアプリケーションで単一の共有データベースに保持されるようにする。

部門。

D. システムで注文が処理される前に重複を検出するために、照合制御を実装します。

Answer: C ([メッセージを残す](#))

セクション : 情報資産の保護

Explanation:

データを一箇所に保管することは、データが重複なく保存され、すべてのデータがユーザーはシステム上に同じデータを持っています。頻度を増やすことで、

問題点としては、並行してデータ入力が行われる可能性があるため、重複のリスクを完全に排除することはできない。

ビジネス要件によって、データ処理活動が行われる場所が決まる可能性が高い。

IT問題を解決するためのビジネス構造は、実用的でも政治的にも実現可能ではない。検出制御は重複処理の問題を解決し、追加のプロセスを実装する必要がある

発見された重複データを処理する。

最新問題: 553

分散型サービス拒否 (DDoS) 攻撃が発生していることを最も適切に検知できるのは、次のうちどれですか？

- A. カスタマーサービスに関する苦情
- B. ログの自動監視
- C. サーバーがクラッシュしました
- D. 侵入テスト

Answer: B ([メッセージを残す](#))

分散型サービス拒否 (DDoS) 攻撃が発生していることを検出する最善の方法は、ログの自動監視を使用することです。DDoS攻撃は、不要なインターネットトラフィックを大量にサーバー、サービス、またはネットワークに送り込むことで、それらの運用を妨害します²。ログの自動監視は、ネットワークトラフィックパターンを分析し、トラフィックの急増やその他の異常なアクティビティを監視し、異常や悪意のあるリクエスト、プロトコル、またはIPブロックについて管理者やセキュリティチームに警告することで、潜在的なDDoS攻撃を特定するのに役立ちます³。ログの自動監視は、DDoS攻撃の発生源、種類、および影響を特定し、さらなる調査や軽減のための証拠を提供するのにも役立ちます。

他のオプションは、DDoS 攻撃を検出するためのログの自動監視ほど効果的ではありません。カスタマー サービスへの苦情は、ユーザーが Web サイトやサービスへのアクセスに関する問題を報告することに依存するため、DDoS 攻撃の間接的かつ遅延的な指標となります。カスタマー サービスへの苦情は、サーバー エラーやネットワークの問題など、DDoS 攻撃とは無関係の他の要因によっても発生する可能性があります。サーバーのクラッシュは、サーバーがすでに攻撃によって過負荷になり、機能を停止していることを示すため、DDoS 攻撃の極端で望ましくない指標です。サーバーのクラッシュは、データの損失や破損、サービスの中断、評判の低下につながる可能性もあります。侵入テストは、システムまたはネットワークのセキュリティ スタンスを評価するための積極的かつ予防的な措置ですが、進行中の DDoS 攻撃を検出しません。侵入テストでは、システムまたはネットワークの回復力または脆弱性をテストするために DDoS 攻撃をシミュレートすることがありますが、リアルタイムのトラフィックを監視したり、実際の攻撃者を特定したりすることはありません。

参考文献：

- * ISACA CISAレビューマニュアル第27版 (2019年)、254ページ
- * DDoS攻撃を防ぐ方法 | 方法とツール | Cloudflare²
- * サービス拒否攻撃の理解 | CISA³

最新問題: 554

IS監査担当者は、80%以上完了しているものの、既に工期が10%、コストが25%超過しているソフトウェア開発プロジェクトの監査を担当することになった。IS監査担当者は、次のうちどの行動を取るべきだろうか？

- A. 組織には効果的なプロジェクト管理がないと報告する。
- B. プロジェクトマネージャーの変更を推奨します。
- C. ITガバナンス構造を見直す。
- D. プロジェクトの実施状況とビジネスケースをレビューする。

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

IS監査担当者は、勧告を行う前に、プロジェクトの内容と、予算超過やスケジュール超過の原因となった要因を理解する必要があります。組織は効果的なプロジェクト管理手法と健全なITガバナンス体制を備えていても、スケジュール遅延や予算超過に陥る可能性があります。予算超過の原因を調査せずにプロジェクトマネージャーを交代させるべき理由は何もありません。

最新問題: 555

The PRIMARY reason an IS department should analyze past incidents and problems is to:

- A. determine if all incidents and problems are reported.
- B. assign responsibility for problems.
- C. assess help desk performance.
- D. identify the causes of recurring incidents and problems.

Answer: ([解答を表示する](#))

Section: Protection of Information Assets

最新問題: 556

IT監査組織における役割と責任を定義する文書として、次のうちどれが適切でしょうか？

- A. 監査憲章
- B. 年間監査計画
- C. 婚約書
- D. 監査範囲に関する書簡

Answer: ([解答を表示する](#))

包括的かつ詳細な手順説明：

監査憲章とは、内部監査機能の目的、権限、および責任を定義する正式な文書である。

* 監査憲章（正解 A）

監査チームの役割、報告体制、および独立性を確立する。

* 例: IS監査チームのリスク評価における役割は、憲章に概説されています。

* 年次監査計画（誤） - B）

* 監査活動の概要は示しているが、役割と責任は定義していない。

* 婚約書（誤） - C）

* 特定の監査に使用され、監査機能全体には使用されません。

* 監査範囲に関する書簡（誤） - D）

* 監査の対象となる内容を詳述するが、責任範囲を定義するものではない。

参考文献：

* ISACA CISAレビューマニュアル

* COBIT 2019（監査ガバナンス）

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 557

ITサービスの可用性と継続性を確保するためのITのベストプラクティスは、以下の点を満たすべきである。

- A. 災害に強いコンポーネントに関連するコストを最小限に抑える。
- B. 事業の合意された需要を満たすのに十分な能力を提供する。
- C. 顧客との合意された義務が履行できることを合理的に保証する。
- D. タイムリーなパフォーマンス指標レポートを作成する。

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

交渉され合意されたコミットメント すなわち、サービスレベル契約 [SLA] が常に履行できることが重要です。これが実現不可能であれば、IT はこれらの要件に同意すべきではありませんでした。なぜなら、そのようなコミットメントを行うことはビジネスを誤解させることになるからです。この文脈における「常に」とは、「合意された義務」に直接関係し、サービスが 100% の時間利用可能でなければならないという意味ではありません。コストは可用性とサービス継続性管理の結果であり、部分的にしか制御できない場合があります。これらのコストは、合意された義務を直接反映しています。キャパシティ管理は可用性の必要条件ですが、十分条件ではありません。キャパシティ不足が可用性の問題につながる可能性があっても、サービスのシームレスな運用に必要なキャパシティの提供は、可用性管理ではなく、キャパシティ管理で行われます。レポートの生成は可用性とサービス継続性管理のタスクである可能性がありますが、これは他の多くの関心領域 (インシデント、問題、キャパシティ、変更管理など) にも当てはまります。

最新問題: 558

IS監査マネージャーは、同じマネージャーが監査した監査の品質レビューを行うよう依頼された。監督下にある。この状況に対するマネージャーの最も適切な対応は次のうちどれですか？

- A. 監査委員会に状況を報告してください。
- B. 監査部門の上級幹部に状況を報告してください。
- C. 監査証拠が監査結論を裏付けているかどうかを判断する。
- D. 監査チームと話し合っ、どのようにして結論に至ったのかを理解してください。

Answer: ([解答を表示する](#)**)**

セクション：情報システムの監査プロセス

最新問題: 559

ウェブサーバー上に存在するオペレーティングシステムユーティリティによって実行される可能性が最も高い機能はどれですか？

- A. ネットワークプロトコルの設定
- B. 端末の警告メッセージとエラーメッセージの送受信
- C. POS端末などの端末機器の制御合計を生成する
- D. 利用状況とトラフィックパターンの監視

Answer: D ([メッセージを残す](#))

最新問題: 560

An IS auditor is verifying the adequacy of an organization's internal controls and is concerned about potential circumvention of regulations. Which of the following is the BEST sampling method to use?

- A. Variable sampling
- B. Cluster sampling
- C. Attribute sampling
- D. Random sampling

Answer: C ([メッセージを残す](#))

最新問題: 561

サイバー攻撃が発生した際に、拡散のリスクを軽減できるセキュリティ対策は次のうちどれですか？

- A. Webアプリケーションファイアウォール (WAF)
- B. データ損失防止 (DLP) システム
- C. ネットワーク分割
- D. 外周ファイアウォール

Answer: C ([メッセージを残す](#))

最新問題: 562

.What should an IS auditor do if he or she observes that project-approval procedures do not exist?

- A. Advise senior management to invest in project-management training for the staff
- B. Create project-approval procedures for future project implementations
- C. Assign project leaders
- D. Recommend to management that formal approval procedures be adopted and documented

Answer: D ([メッセージを残す](#))

If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and documented.

最新問題: 563

Internal audit reports should be PRIMARILY written for and communicated to:

- A. audit management as they are responsible for the quality of the audit.
- B. senior management as they should be informed about the identified risks.
- C. external auditors, as they provide an opinion on the financial statements.
- D. auditees, as they will eventually have to implement the recommendations

Answer: B ([メッセージを残す](#))

最新問題: 564

Which of the following should be of GREATEST concern to an IS auditor reviewing on-site preventive maintenance for an organization's business critical server hardware?

- A. Preventive maintenance costs exceed the business's allocated budget
- B. The preventive maintenance schedule is based on mean time between failures (MTBF) parameters
- C. Preventive maintenance has not been approved by the information system owner
- D. Preventive maintenance is outsourced to multiple vendors without requiring nondisclosure agreements

Answer: D ([メッセージを残す](#))

(NDAs)

最新問題: 565

IS監査担当者が、組織の正式な事業継続計画の策定に参加するよう依頼された。
プログラム。次のうち、監査人の独立性を損なうものはどれですか？

- A. 災害復旧テストシナリオの開発
- B. システムの重要度判定
- C. 事業影響分析 (BIA)の促進
- D. 事業継続委員会への参加

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

最新問題: 566

Using the OSI reference model, what layer(s) is/are used to encrypt data?

- A. transport layer
- B. Session layer
- C. Session and transport layers
- D. Data link layer

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

User applications often encrypt and encapsulate data using protocols within the OSI session layer or farther down in the transport layer.

最新問題: 567

監査を計画する際、IS監査人がサービスレベル管理に関するサードパーティプロバイダーの外部監査レポートに依拠することは許容されます。

- A. 報告書は、サービス水準が侵害されていないことを確認した。
- B. 過去12ヶ月以内に発表されたレポート
- C. サービス提供者は独立した認証および認定を受けています
- D. 範囲と方法論が監査要件を満たしている

Answer: ([解答を表示する](#))

最新問題: 568

Which of the following is the GREATEST security risk associated with data migration from a legacy HR system to a cloud-based system?

- A. System performance may be impacted by the migration.
- B. Records past their retention period may not be migrated to the new system.
- C. ソースシステムとターゲットシステムのデータは、データ形式が異なる場合があります。
- D. 送信元および送信先システムのデータが傍受される可能性があります。

Answer: D ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 569

Which of the following findings is the GREATEST concern when reviewing a disaster recovery plan (DRP) with high availability requirements?

- A. Annual tabletop testing is not required.
- B. Recovery time objectives (RTOs) are not defined.
- C. Vendor contact information is not reviewed.
- D. Responsibilities are not defined for the recovery team.

Answer: B ([メッセージを残す](#))

最新問題: 570

小規模なeコマース企業の経営陣は、AIの導入が自社の知的財産に与える影響を懸念している。この懸念に最も適切に対応できるのは次のうちどれか？

- A. AIの許容利用ポリシーの策定
- B. 生成型AIを使用した従業員への制裁
- C. AIウェブトラフィックログの手動レビューの実施
- D. チャットベースのAIウェブサイトとプラグインを拒否リストに追加する

Answer: A ([メッセージを残す](#))

包括的かつ詳細な説明：

最善のアプローチは、従業員が機密情報や知的財産を保護しながらAIツールをどのように使用できるかを明確に定義した、AIの適切な利用に関するポリシーを策定することです。これにより、ガバナンスを確保しつつ、安全な導入が可能になります。

* オプションB：事後対応型で懲罰的な統治であり、事前対応型の統治ではない。

* オプションC：モニタリングは役立つが、それだけでは不十分である。

* オプションD：過度に制限的であり、有益なAIの利用を妨げる可能性がある。

* オプションA：正解 ポリシーは、事業目標とリスク管理に沿った体系的なガイダンスを提供します。

ISACA 参考資料: AI ガバナンス、リスク、コンプライアンスに関する ISACA ホワイトペーパー; CISA レビュー マニュアル 第27版、ドメイン1、政策枠組みと新興技術に関するセクション。

最新問題: 571

組織内での未承認ソフトウェアの使用に関して、最も懸念される事項は次のうちどれですか？

- A. 社内IT手順の遵守不足
- B. 非効率的なITサポートとメンテナンス
- C. データ漏洩およびセキュリティ侵害のリスク
- D. ソフトウェアライセンスおよびサブスクリプションのコスト増加

Answer: ([解答を表示する](#))

承認されていない（無許可の）ソフトウェアに関する最大の懸念は、データ漏洩やセキュリティ侵害の可能性です。このようなソフトウェアは、適切なセキュリティ対策が欠如していたり、脆弱性を含んでいたりと、組織の監視を回避したりする可能性があり、データの機密性、完全性、およびシステムセキュリティに重大なリスクをもたらします。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **572**

ITガバナンスおよび管理の監査において、以下の所見のうちどれが最も懸念すべきでしょうか？

- A. IT戦略策定プロセスが文書化されていない。
- B. 事業戦略委員会の会議にIT部門の代表者がいない。
- C. 組織は国際的なIT管理基準に準拠していません。
- D. 最高情報セキュリティ責任者 (CISO)の役職はありません。

Answer: B ([メッセージを残す](#))

最新問題: **573**

Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

- A. Degaussing
- B. Overwrite every sector of magnetic media with pattern of 1's and 0's
- C. Format magnetic media
- D. Delete File allocation table

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Software tools can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media.

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed. Simply deleting files or formatting media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides.

Specialized hardware devices known as degausses can be used to erase data saved to magnetic media.

The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object

reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There exists a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back- and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. To provide higher assurance in this case, it is necessary to overwrite each sector multiple times. Security practitioners should keep in mind that a one- time pass may be acceptable for noncritical information, but sensitive data should be overwritten with multiple passes. Overwrite software can also be used to clear the sectors within solid-state media such as USB thumb drives. It is suggested that physical destruction methods such as incineration or secure recycling should be considered for solid-state media that is no longer used.

The last form of preventing unauthorized access to sensitive data is media destruction. Shredding, burning, grinding, and pulverizing are common methods of physically destroying media. Degaussing can also be a form of media destruction. High-power degausses are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal.

The following answers are incorrect:

Degaussing -Erasing data by applying magnetic field around magnetic media. Degausses device is used to erase the data.

Sometime degausses can make magnetic media unusable. So degaussing is not recommended way if magnetic media needs to be reused.

磁気メディアのフォーマット - 磁気メディアをフォーマットしても、すべてのデータが消去されるわけではありません。フォーマット後でも、ソフトウェアツールを使用すればデータを復元できます。

ファイル割り当てテーブルを削除しても、すべてのデータが消去されるわけではありません。ソフトウェアツールを使用すれば、データを復元できる場合があります。

参照：

CISAレビューマニュアル2014年版 338ページ

最新問題: 574

組織が内部ネットワークに保存されているデータを分類する主な理由は何ですか？

- A. データ保持ポリシーを決定する
- B. データ保護要件を実施する
- C. 組織のデータポリシーを遵守するため
- D. 業界のベストプラクティスに従う

Answer: ([解答を表示する](#))

組織が内部ネットワークに保存されているデータを分類する主な理由は、データ保護要件を実装するためです1234。データ分類は、組織がどのようなデータを持っているか、その特性、必要な保護を実現するために満たすべきセキュリティとプライバシーの要件を理解するのに役立ちます3。データ保持ポリシーの決定56、組織のデータポリシーの遵守27、業界のベストプラクティス891011の遵守はデータ分類の重要な側面ですが、データ保護要件を実装するという基本的な要件に比べると二次的なものです。
参考文献：

データ分類とは何か、そしてなぜ重要なのか？ - RiskOptics

データ分類ポリシー：定義例、無料テンプレート - Hyperproof データ分類ポリシー：メリット、例、テクニック - Satori データ分類ポリシーとは？ - Digital Guardian データ分類と実践 - NIST データ分類はデータ保持とアーカイブの触媒となる...

データ分類とは何か？ - クラウド導入フレームワーク

データ分類 - データセキュリティポリシー | ITSポリシー...

データ分類の実践の実施 - NIST

データ分類のベストプラクティス | Forcepoint

最新問題: 575

IS監査担当者は、機密レポートをオフライン印刷用にスプールすることに伴うリスクを考慮すると、最も懸念される点：

- A. オペレーターがデータを簡単に読み取ることができます
- B. データは権限のない者によって容易に改ざんされる可能性がある
- C. 報告書の無断コピーを印刷できます
- D. システムが故障した場合、出力は失われます

Answer: C ([メッセージを残す](#))

セクション：情報システムの監査プロセス

最新問題: 576

Which of the following provides for the GREATEST cost reduction in a large data center?

- A. Server consolidation
- B. Staff rotation
- C. Power conditioning
- D. Job-scheduling software

Answer: A ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: 577

An IS auditor finds a segregation of duties issue in an enterprise resource planning (ERP) system. Which of the following is the BEST way to prevent the misconfiguration from recurring?

- A. Monitoring access rights on a regular basis
- B. Referencing a standard user-access matrix
- C. Granting user access using a role-based model
- D. Correcting the segregation of duties conflicts

Answer: C ([メッセージを残す](#))

Explanation

The best way to prevent the misconfiguration from recurring is to grant user access using a role-based model. A role-based access control (RBAC) model is an access control method that assigns permissions to end-users based on their role within the organization¹. RBAC provides fine-grained control, offering a simple, manageable approach to access management that is less error-prone than individually assigning permissions¹. RBAC also enforces the principle of least privilege, which means that users only have the minimum access required to perform their tasks².

A role-based model can help prevent segregation of duties (SoD) issues in an ERP system by restricting user access to conflicting activities within the application. SoD is a central issue for enterprises to ensure compliance with laws and regulations, and to reduce the risk of fraud and unauthorized transactions³. SoD requires that no single individual or group of individuals should have control over two or more parts of a process or an asset³. For example, a user who can create and approve purchase orders should not be able to process payments or modify vendor records.

By using a role-based model, user access provisioning is based on the needs of a group (e.g., accounting department) based on common responsibilities and needs¹. This means each role has a given set of permissions, and individuals can be assigned to one or more roles. For example, you may designate a user as an accounts payable clerk, an accounts receivable clerk, or a financial manager, and limit access to specific resources or tasks. The user-role and role-permissions relationships make it easy to perform role assignment because individual users no longer have unique access rights, rather they have privileges that conform to the permissions assigned to their specific role or job function¹.

The other options are not the best way to prevent the misconfiguration from recurring. Monitoring access rights on a regular basis (option A) is a detective control that can help identify SoD issues after they occur, but it does not prevent them from happening in the first place. Referencing a standard user-access matrix (option B) is a tool that can help document and analyze user access rights, but it does not ensure that the user access rights are configured correctly or consistently. Correcting the segregation of duties conflicts (option D) is a corrective action that can resolve SoD issues once they are detected, but it does not prevent them from happening again.

References: 3: Implementing Segregation of Duties: A Practical Experience Based on Best Practices 1: What is Role-Based Access Control (RBAC)? Examples, Benefits, and More 2: What is Azure role-based access control (Azure RBAC)?

最新問題: 578

During the implementation of an enterprise resource planning (ERP) system, an IS auditor is reviewing the results of user acceptance testing (UAT). The auditor's PRIMARY focus should be to determine if:

- A. all errors found in the testing process have been corrected.
- B. application interfaces have been satisfactorily tested.
- C. the business process owner has signed off on the results.
- D. system integration testing was performed.

Answer: A ([メッセージを残す](#))

最新問題: 579

OSI参照モデルにおいて、データの暗号化にはどの層が使用されますか？

- A. トランスポート層
- B. セッション層
- C. セッション層とトランスポート層
- D. データリンク層

Answer: C ([メッセージを残す](#))

説明／参考資料：

ユーザーアプリケーションは、OSIセッション層内、あるいはトランスポート層のさらに下位層にあるプロトコルを使用して、データを暗号化およびカプセル化することがよくあります。

最新問題: 580

ITバランススコアカードは、以下の項目を監視するための最も効果的な手段です。

- A. 制御効果。
- B. 投資収益率 (ROI)。
- C. 企業ITのガバナンス。
- D. 変革管理の有効性。

Answer: C ([メッセージを残す](#))

最新問題: 581

事業継続計画 (BCP) のテストにおいて、以下の結果分析方法のうち、計画が実行可能であることを最も確実に保証できるのはどれですか？

- A. 精度測定
- B. 重要タスクの完了に要した経過時間
- C. テスト結果を定量的に測定する
- D. 観察された試験結果の評価

Answer: C ([メッセージを残す](#))

説明／参考資料：

計画の成功度を測り、明示された目標に対するテストを実施する方法を持つことが重要です。

したがって、結果は観察のみに基づく評価ではなく、定量的に測定されなければならない。

テスト結果を定量的に測定するには、BCP中に実施されたすべての活動を測定する包括的な記述が必要であり、これにより効果的な計画であることを最も確実に保証できます。選択肢AとBも定量的な指標ではありますが、特定の領域、あるいは結果の正確性や経過時間といった一点からの分析に関するものです。

出典：情報システム監査 統制協会、公認情報システム監査人2002年版レビューマニュアル、第5章：災害復旧と事業継続 269ページ)。

最新問題: 582

Which of the following would be the BEST access control procedure?

- A. The data owner formally authorizes access and an administrator implements the user authorization tables.
- B. Authorized staff implements the user authorization tables and the data owner sanctions them.
- C. The data owner and an IS manager jointly create and update the user authorization tables.
- D. The data owner creates and updates the user authorization tables.

Answer: (解答を表示する)

The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

最新問題: 583

The PRIMARY objective of value delivery in reference to IT governance is to:

- A. promote best practices
- B. increase efficiency.
- C. optimize investments.
- D. ensure compliance.

Answer: C ([メッセージを残す](#))

The primary objective of value delivery in reference to IT governance is to optimize investments. Value delivery is one of the five focus areas of IT governance that aims to ensure that IT delivers expected benefits to stakeholders and enables business value creation. Value delivery involves aligning IT investments with business objectives and strategies, managing IT performance and benefits realization, optimizing IT costs and risks, and enhancing IT innovation and agility. Value delivery helps to maximize the return on investment (ROI) and value for money (VFM) of IT resources and capabilities. References:

* CISA Review Manual (Digital Version)

* CISA Questions, Answers & Explanations Database

最新問題: 584

以下の消火システムのうち、作動時に電力供給を遮断する自動スイッチと組み合わせる必要があるのはどれですか？

- A. 二酸化炭素
- B. FM-200
- C. 乾いたパイプ
- D. ハロン

Answer: A ([メッセージを残す](#))

説明

二酸化炭素消火システムは、作動時に自動的に電源を遮断するスイッチと組み合わせる必要があります。これは、二酸化炭素が空気中の酸素を置換し、保護区域内の人々に窒息の危険をもたらす可能性があるためです。したがって、感電や火花による再燃を防ぐため、二酸化炭素を放出する前に電源を遮断することが不可欠です。

二酸化炭素システムは、サーバー室やデータセンターなど、居住に適さない空間における全面的な空気充满用途に一般的に使用されます。

最新問題: 585

多国籍企業が、データ保護とプライバシーを含む情報セキュリティに関する強制的なグローバル標準を確立しようとしている。情報セキュリティ監査担当者にとって、以下のうちどれが最も懸念すべき事項だろうか？

- A. 関係国における現地法の不遵守
- B. 影響を受けるすべての国で、組織化された労働団体による採用が不足している。
- C. 目に見える成果のない組織的な努力の増加
- D. 各国で規格の導入状況にばらつきがある

Answer: A ([メッセージを残す](#))

最新問題: 586

Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

- A. System flowchart
- B. Data flow diagram
- C. Process flowchart
- D. Entity-relationship diagram

Answer: C ([メッセージを残す](#))

The best document for an IS auditor to use in detecting a weakness in segregation of duties is a process flowchart. A process flowchart is a diagram that illustrates the sequence of steps, activities, tasks, or decisions involved in a business process. A process flowchart can help detect a weakness in segregation of duties by showing who performs what actions or roles in a process, and whether there is any overlap or conflict of interest among them. The other options are not as useful as a process flowchart in detecting a weakness in segregation of duties, as they do not show who performs what actions or roles in a process. A system flowchart is a diagram that illustrates the components, functions, interactions, or logic of an information system. A data flow diagram is a diagram that illustrates how data flows from sources to destinations through processes, stores, or external entities. An entity-relationship diagram is a diagram that illustrates how entities (such as tables) are related to each other through attributes (such as keys) in a database. References: CISA ReviewManual (Digital Version), Chapter 3, Section 3.2

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **587**

Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

- A. Assess the impact of patches prior to installation.
- B. Ask the vendors for a new software version with all fixes included.
- C. install the security patch immediately.
- D. Decline to deal with these vendors in the future.

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions with all fixes included are not always available and a full installation could be time consuming. Declining to deal with vendors does not take care of the flaw.

最新問題: **588**

データセンターにおける物理的な情報資産の保護にとって、最も重要な前提条件は次のうちどれですか？

- A. 展開済みの情報資産の完全かつ正確なリスト

- B. 現場設置型バックアップ発電機の可用性とテスト
- C. 屋台の発注と屋台の受領に関する情報資産間の職務分掌
- D. データ保護要件に関するITスタッフの知識

Answer: D ([メッセージを残す](#))

最新問題: 589

Which of the following is the MOST important difference between end-user computing (EUC) applications and traditional applications?

- A. Traditional application documentation is typically less comprehensive than EUC application documentation.
- B. Traditional applications require roll-back procedures whereas EUC applications do not.
- C. Traditional applications require periodic patching whereas EUC applications do not.
- D. Traditional application input controls are typically more robust than EUC application input controls.

Answer: D ([メッセージを残す](#))

最新問題: 590

新しい情報システムが本番環境への移行準備が整っていることを最も確実に保証できるのは、次のうちどれですか？

- A. 社内チームによるシステム品質保証 (QA)
- B. 変更諮問委員会の承認
- C. 開発チームが実施した侵入テストの結果
- D. エンドユーザー受け入れテスト (UAT)の結果

Answer: D ([メッセージを残す](#))

最新問題: 591

Which of the following is the PRIMARY benefit of leveraging an IT-related framework when conducting an audit?

- A. It provides a comprehensive list of potential audit findings.
- B. It provides a standardized model for the audit subject.
- C. It ensures alignment with audit standards.
- D. It supports the credibility of the audit report.

Answer: B ([メッセージを残す](#))

Using an established IT-related framework (such as COBIT or ISO/IEC 27001) gives the IS auditor a structured and standardized model to assess controls, processes, and governance. This ensures consistent evaluation criteria and improves the reliability and comparability of audit results.

最新問題: 592

Which of the following BEST determines if a batch update job was successfully executed?

- A. Testing a sample of transactions to confirm updates were applied
- B. Reviewing a copy of the script for the job
- C. Obtaining process owner confirmation that the job was completed
- D. Verifying the timestamp from the job log

Answer: ([解答を表示する](#))

最新問題: 593

データ分類プロジェクトを実施する際、情報セキュリティ管理者は以下のことを行うべきです。

- A. 情報の批判的および機密性を割り当てる
- B. 情報所有者を特定する
- C. 情報管理者の特定
- D. 情報アクセス権限を割り当てる

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

最新問題: 594

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

- A. Blowfish
- B. Tripwire
- C. certificate
- D. DES
- E. one-time pad
- F. None of the choices.

Answer: E ([メッセージを残す](#))

Explanation/Reference:

Explanation:

It's possible to protect messages in transit by means of cryptography. One method of encryption - the one- time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

最新問題: 595

インターネットの電子商取引サイトで、ホスティングサーバーに1つの秘密鍵があり、公開鍵が顧客に広く配布されている非対称暗号化を使用することは、最も安心感を与える可能性が高いのは、次の点です。

- A. ホスティング組織の信頼性に関する顧客。
- B. 顧客の信頼性に関するホスティング組織。
- C. ホスティング組織からのメッセージの機密性に関する顧客。
- D. 顧客に渡されるメッセージの機密性に関するホスティング組織。

Answer: (解答を表示する)

説明／参考資料：

Explanation:

偽サイトは正規サイトの秘密鍵を使用して暗号化することができないため、顧客は公開鍵を使用してメッセージを復号化することはできません。多くの顧客が同じ公開鍵にアクセスできるため、ホストはこの仕組みを使用して顧客の認証を保証することはできません。多くの人が公開鍵にアクセスしてホストからのメッセージを復号化できるため、顧客はホストからのメッセージの

機密性を保証することができません。多くの人が公開鍵にアクセスして復号化できるため、ホストは送信されたメッセージの機密性を保証することができません。

最新問題: **596**

組織のIT資産への投資計画と管理の有効性を理解するために、IS監査人は以下の点をレビューする必要があります。

- A. エンタープライズデータモデル。
- B. ITバランススコアカード (BSC)
- C. IT組織構造。
- D. 過去の財務諸表。

Answer: B ([メッセージを残す](#))

ITバランススコアカード (BSC)は、従来の財務評価に顧客満足度、内部プロセス、イノベーション能力を評価する指標を追加することで、IT目標とビジネス目標の間の橋渡しをするツールです。エンタープライズデータモデルは、組織のデータ構造とデータの相互関係を定義する文書です。これは有用ですが、投資に関する情報は提供しません。IT組織構造は、ITエンティティ内の機能関係と報告関係の概要を提供します。過去の財務諸表は計画に関する情報を提供せず、IT資産に関する経営陣の活動を完全に理解するのに十分な詳細がありません。過去のコストは必ずしも価値を反映しているとは限らず、データなどの資産は会計帳簿に表されません。

最新問題: **597**

Which of the following would BEST prevent data from being orphaned?

- A. Referential integrity
- B. Table partitioning
- C. Input validation checks
- D. Table indexes

Answer: A ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

Explanation/Reference:

最新問題: **598**

When auditing a software development project, a review of which of the following will BEST verify that project work is adequately subdivided?

- A. Work breakdown structure
- B. Statement of work
- C. Scope statement
- D. Functional and technical design documents

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation

最新問題: **599**

Which of the following should be an IS auditor's GREATEST concern when evaluating a cybersecurity incident response plan?

- A. The plan does not include incident response metrics
- B. The plan has not been recently tested
- C. Rules and responsibilities are not detailed for each process
- D. Stakeholder contact details are not up to date

Answer: A ([メッセージを残す](#))

最新問題: 600

ホットサイトの契約交渉において、最も重要な懸念事項は次のうちどれですか？

- A. 複数の災害宣言が出された場合のサイトの可用性
- B. 複数の災害宣言が出された場合の現場スタッフとの連携
- C. 他組織との相互協定
- D. 復旧計画のテストを完了する

Answer: A ([メッセージを残す](#))

ホットサイト契約の交渉において最も重要な懸念事項は、複数の災害宣言が発生した場合に、そのサイトが利用可能であるかどうかです。ホットサイトとは、災害発生時に事業運営を再開するために使用できる、設備が整った代替施設のことです。しかし、ホットサイト提供業者の複数の顧客が同時に災害を宣言した場合、すべての顧客に対応できるだけの資源やキャパシティが不足する可能性があります。

Therefore, the contract should specify the terms and conditions for ensuring the availability and priority of the hot site for the organization. The other options are not as important as availability, as they do not affect the ability to use the hot site in a disaster situation. Coordination with the site staff in the event of multiple disaster declarations is a logistical issue that can be resolved by communication and planning. Reciprocal agreements with other organizations are alternative arrangements that can be used to share resources or facilities in a disaster, but they may not be as reliable or suitable as a hot site. Complete testing of the recovery plan is a good practice that can help validate and improve the effectiveness of the recovery plan, but it is not a concern for negotiating a contract for a hot site. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3

最新問題: 601

The reason a certification and accreditation process is performed on critical systems is to ensure that:

- A. security compliance has been technically evaluated.
- B. data have been encrypted and are ready to be stored.
- C. the systems have been tested to run on different platforms.
- D. the systems have followed the phases of a waterfall model.

Answer: A ([メッセージを残す](#))

Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 602

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

- A. registration authority (RA).
- B. certificate authority (CA).
- C. certificate repository.
- D. receiver.

Answer: B ([メッセージを残す](#))

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

最新問題: 603

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

- A. True
- B. False

Answer: ([解答を表示する](#)**)**

Explanation/Reference:

Explanation:

An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

最新問題: 604

ある組織が、機密データが電子メールを介して組織外に流出するリスクを軽減するための対策として、データ損失防止ツールを導入しました。以下のうち、適切な制御設計を示す最良の指標となるのはどれでしょうか？

- A. 経営陣は制御設計を正式に承認しました。
- B. 経営陣は、データ損失事故が減少したことを示す証拠を提示する。
- C. セキュリティ管理者は、ツールの機能を実演できます。
- D. このツールによって適用されるルールは、データの分類に基づいていました。

Answer: ([解答を表示する](#)**)**

セクション: 情報システムの取得、開発、導入

最新問題: 605

企業データ分類プログラムを成功裏に導入するための最初のステップとして、次のうちどれが適切でしょうか？

- A. データ分類ポリシーを承認する。
- B. データ損失防止 (DLP) プロトコルを選択します。
- C. 必要な規制要件を確認してください。
- D. プロジェクトに必要なリソースが十分に確保されていることを確認してください。

Answer: C ([メッセージを残す](#))

最新問題: 606

During a project assessment, an IS auditor finds that business owners have been removed from the project initiation phase. Which of the following should be the auditor's GREATEST concern with this situation?

- A. Unrealistic milestones
- B. Inadequate deliverables
- C. Unclear benefits
- D. Incomplete requirements

Answer: D ([メッセージを残す](#))

正解はDです。IS監査担当者にとって、事業責任者がプロジェクト開始段階から除外される状況で最も懸念されるのは、要件が不完全になる可能性があることです。プロジェクト開始段階は、新しいプロジェクトを開始する最初のステップであり、プロジェクトの目的、範囲、目標、成果物が定義され、文書化されます。また、プロジェクト開始段階では、スポンサー、顧客、ユーザー、事業責任者など、プロジェクトに関心や影響力を持つ主要なステークホルダーを特定し、関与させることも含まれます。

事業主とは、プロジェクトにおける事業ニーズと期待値を定義する権限と責任を持つ個人または組織のことです。また、事業主はプロジェクトの成果と利益の主要な受益者でもあります。事業主は、プロジェクトの要件と仕様に関する貴重な意見やフィードバックを提供するため、プロジェクト開始段階で重要な役割を果たします。要件とは、事業ニーズと期待値を満たすためにプロジェクトが達成すべきこと、または提供すべきものを記述したものです。要件は、プロジェクトの計画、実行、監視、および完了の各段階を導く上で不可欠です。

プロジェクト開始段階から事業責任者が排除されると、要件が不完全または不正確になり、プロジェクトの品質、範囲、時間、コスト、リスクに悪影響を及ぼす可能性があります。要件が不完全になった場合に起こりうる結果には、以下のようなものがあります。

- * 不整合 :プロジェクトが事業戦略、ビジョン、または目標と一致しない場合、その価値や関連性が低下する可能性があります。
- * 混乱 :プロジェクトチームがプロジェクトで達成すべきことや提供すべきものを明確に理解していない可能性があります、それがパフォーマンスや生産性に影響を与える可能性があります。
- * 手戻り :プロジェクトは、新しい要件や変更された要件に対応するために、頻繁な変更や修正が必要になる場合があります、その結果、プロジェクトの時間とコストが増加する可能性があります。
- * 不満 :プロジェクトが事業主やその他の利害関係者の期待や満足度を満たさない可能性があります、それがプロジェクトの受容や支持に影響を与える可能性があります。
- * 失敗 :プロジェクトが期待される成果や利益をもたらさない可能性があります、その成功や存続可能性に影響を与える可能性があります。

したがって、IS監査人は、プロジェクト開始段階における事業責任者の関与と参加について注意を払うべきです。なぜなら、それは要件の完全性と品質に影響を与えるからです。IS監査人は、利害関係者の特定と関与に関する方針と手順を確認し、事業責任者が要件を定義するのに十分な知識とスキルを持っていることを確認し、要件が適切に定義され、文書化され、承認され、伝達されていることをテストする必要があります。

参考文献 :

Project Initiation: The First Step to Project Management [2023] * Asana Everything you need to know about the project initiation phase Project Initiation Phase - The Business Professor Project Initiation: A Guide to Starting a Project Right Way - Kissflow

最新問題: **607**

Who should be the FIRST to evaluate an audit report prior to issuing it to the project steering committee?

- A. Audit committee
- B. Business owner
- C. Project sponsor
- D. IS audit manager

Answer: D ([メッセージを残す](#))

The IS audit manager should be the first to evaluate an audit report before it is issued to the project steering committee. This ensures the report's accuracy, completeness, and alignment with audit objectives. The audit manager reviews findings, conclusions, and recommendations to maintain quality and professionalism in the audit deliverable.

最新問題: **608**

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- A. Personal firewall
- B. Antivirus programs
- C. Intrusion detection system (IDS)
- D. Virtual local area network (VLAN) configuration

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

An intrusion detection system (IDS) would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator. Antivirus programs, personal firewalls and VIAN configurations would be later in the line of defense.

最新問題: **609**

The results of a feasibility study for acquiring a new system should provide management with a clear understanding of:

- A. the approach to meeting data processing needs.
- B. how hardware selection criteria are aligned with the IS strategic plan.
- C. critical application systems' utilization of computer resources.
- D. application security over critical data processing.

Answer: A ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: **610**

An IS auditor is reviewing job scheduling software and notes instances of delayed processing time, unexpected job interruption, and out-of-sequence job execution. Which of the following should the auditor examine FIRST to help determine the reasons for these instances?

- A. System schedule
- B. Job schedule
- C. Exception log
- D. Change log

Answer: C ([メッセージを残す](#))

The exception log should be examined first, as it provides detailed records of errors, failures, or anomalies in the job scheduling process. This log can help the IS auditor identify specific issues causing delayed processing times, job interruptions, or out-of-sequence execution. It offers insights into the root causes and patterns of the incidents, enabling further investigation into related controls or configurations.

最新問題: 611

大規模金融機関に対する継続監査において、以下のうちどれが最適なプロセスでしょうか？

- A. 災害復旧システムにおける暗号化規格のテスト
- B. システム間での並列テストの実施
- C. ヘルプデスク指標のパフォーマンス検証
- D. リアルタイムデータシステムのアクセス制御の検証

Answer: D ([メッセージを残す](#))

最新問題: 612

オープンソースベースのソリューションを使用する最大の利点は、以下の点です。

- A. 明確なサポートレベルが定められている。
- B. 簡単に実装できる。
- C. ベンダーへの依存度を減らす。
- D. より優れたセキュリティ機能を提供する。

Answer: C ([メッセージを残す](#))

包括的かつ詳細な手順説明：

オープンソースソリューションは柔軟性を提供し、ベンダーロックインを軽減するため、組織はソフトウェアを独自に変更、強化、サポートすることができる。

* オプション A (不正解): オープンソースソフトウェアは、構造化された SLA (サービスレベル契約) を提供するプロプライエタリソリューションと比較して、正式なサポートレベルが不足していることが多い。

* オプション B (不正解): オープンソースのソリューションの中には使いやすいものもありますが、実装の複雑さはソフトウェアと必要なカスタマイズによって異なります。

* オプション C (正解): オープンソース ソリューションの主な利点は、ベンダーへの依存から解放されることです。

組織は、特定のベンダーのエコシステムに縛られることなく、ソフトウェアをカスタマイズしたり、独立した開発者を雇用したり、プロバイダーを変更したりすることができる。

* 選択肢 D (誤) オープンソースソフトウェアのセキュリティは、ソリューションを管理するコミュニティと組織に依存します。一部のオープンソースツールは優れたセキュリティを備えていますが、他のツールは追加の強化が必要となる場合があります。

参考資料 :ISACA CISAレビューマニュアル -ドメイン4：情報システム運用と事業継続性-ソフトウェアライセンス、ベンダー依存、およびサポートに関する考慮事項を網羅しています。

最新問題: 613

CAATツールの使用に関して、主な問題点は何ですか？

- A. ソフトウェアベンダーの能力。
- B. 出力のコスト、複雑さ、およびセキュリティの可能性。
- C. 自動化ツールは環境の人間的特性を考慮できない。
- D. 文書による証拠の方が効果的です。

Answer: B ([メッセージを残す](#))

CAAT (コンピュータ支援自動分析技術)は、システムスキャンなどの機能において、人間よりも高速かつ高精度なデータを生成することができる。しかし、コスト、トレーニング、出力のセキュリティが重要な検討事項となる。

最新問題: 614

Which of the following validation techniques would BEST prevent duplicate electronic vouchers?

- A. Cyclic redundancy check
- B. Edit check
- C. Reasonableness check
- D. Sequence check

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

最新問題: 615

An IS auditor is mapping controls to risk for an accounts payable system What is the BEST control to detect errors in the system?

- A. Management approval of payments
- B. Quality control review of new payments
- C. Alignment of the process to business objectives
- D. Input validation

Answer: D ([メッセージを残す](#))

最新問題: 616

IS監査担当者が、組織のリスク管理慣行に関する監査を計画しています。以下のうち、リスク許容度について最も有用な情報を提供するものはどれでしょうか？

- A. リスクポリシー
- B. リスク評価
- C. 過去の監査報告書
- D. 経営上の主張

Answer: A ([メッセージを残す](#))

リスク許容度とは、組織が目標達成のために受け入れるリスクの量と種類のことです。リスク許容度は、組織のリスク文化、戦略、およびリスク耐性を反映し、組織のリスク管理の実践を導きます。リスク許容度に関する最も有用な情報は、リスクポリシーから得られます。リスクポリシーとは、組織のリスク管理フレームワーク、原則、目標、役割、責任、およびプロセスを定義する文

書です。リスクポリシーには、リスクの特定、評価、優先順位付け、軽減、および監視のための基準と閾値、ならびにリスク問題の報告およびエスカレーションメカニズムも定められています。IS監査人は、リスクポリシーをレビューすることで、ポリシーが組織のリスク許容度と整合しているか、一貫性があり包括的であるか、また、リスクを効果的に管理するための明確なガイダンスと方向性を提供しているかどうかを評価できます。

他の選択肢は、最も有用ではないか、リスク許容度とは無関係であるため、正しくありません。

リスク評価とは、組織の目標に影響を与える可能性のあるリスクを特定、分析、評価するプロセスです。リスク評価は、組織の現在のリスクプロファイルとリスクエクスポージャーに関する情報を提供しますが、組織のリスク許容度やリスク選好を示すものではありません。過去の監査報告書は、過去の監査の結果、勧告、結論をまとめた文書です。過去の監査報告書は、組織のリスク管理慣行の過去の実績や問題点に関する情報を提供する場合がありますが、組織のリスク許容度や期待を反映するものではありません。経営陣の表明とは、特定の事実やデータの正確性、完全性、妥当性、信頼性について経営陣が行う声明または宣言です。経営陣の表明は、特定のリスクや問題に関する経営陣の自信や意見に関する情報を提供する場合がありますが、組織のリスク許容度や基準を表すものではありません。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 617

Which of the following line media would provide the BEST security for a telecommunication network?

- A. broadband network digital transmission
- B. Baseband network
- C. Dial-up
- D. Dedicated lines

Answer: D ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

最新問題: 618

次のうち、電子メールのフォーマットをあるネットワークから別のネットワークに変換して、メッセージがすべてのネットワークを通過できるようにするものはどれですか？

- A. ゲートウェイ
- B. プロトコルコンバータ
- C. フロントエンド通信プロセッサ
- D. コンセントレータ／マルチプレクサ

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

ゲートウェイは、電子メールのフォーマットをあるネットワークから別のネットワークに変換する役割を果たし、メッセージがすべてのネットワークを通過できるようにします。

最新問題: 619

.Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

- A. Data diddling
- B. Skimming
- C. Data corruption
- D. Salami attack

Answer: A ([メッセージを残す](#))

Data diddling involves modifying data before or during systems data entry.

最新問題: 620

組織の財務データベースおよび給与データベースに機密レベルを割り当てる責任を主に負うべき役割は、次のうちどれでしょうか？

- A. 情報セキュリティマネージャー
- B. データ所有者
- C. システム管理者
- D. データベース管理者

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

最新問題: 621

Which of the following controls would BEST decrease the exposure if a password is compromised?

- A. Password changes are forced periodically.
- B. Passwords are encrypted.
- C. Passwords are masked.
- D. Passwords have format restrictions.

Answer: ([解答を表示する](#))

最新問題: 622

不正ログインを防止する最も信頼性の高い方法はどれですか？

- A. 認証トークンの発行
- B. 現行のセキュリティポリシーの強化
- C. 営業時間外の利用を制限する
- D. 自動パスワード生成器のインストール

Answer: A ([メッセージを残す](#))

説明

認証トークンの発行は、不正ログインを防止する最も信頼性の高い方法です。認証トークンは、ユーザーがシステムにアクセスするために、所有しているもの（トークン）と知っているもの（個人識別番号またはPIN）の両方を提示する必要があるため、強力な認証形式を提供します。認証トークンは、定期的に変更され、認証サーバーと同期されるワンタイムパスワードまたはコードを生成し、物理デバイスとして機能します。これにより、攻撃者が正当なユーザーの認証情報を盗んだり推測したりすることが困難になります。既存のセキュリティポリシーの強化、営業時間外の使用制限、自動パスワード生成ツールのインストールは、強力な認証形式を提供しないため、認証トークンの発行ほど信頼性が高くなく、不正ログインの試みに対して脆弱なままとなる可能性があります。参考文献：

[認証トークンの定義]

認証 | ISACA

最新問題: 623

A legacy application is running on an operating system that is no longer supported by vendor, if the organization continues to use the current application, which of the application should be the IS auditor's GREATEST concern?

- A. Inability to update the legacy application database
- B. Increased cost of maintaining the system
- C. Inability to use the operating system due to potential licence issues
- D. Potential exploitation of zero-day vulnerabilities in the system

Answer: A ([メッセージを残す](#))

最新問題: 624

As an IS auditor it is very important to understand the importance of job scheduling. Which of the following statement is NOT true about job scheduler or job scheduling software?

- A. Job information is set up only once, which increase the probability of an error.
- B. Records are maintained of all job success and failures.
- C. Reliance on operator is reduced.
- D. Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

Answer: A ([メッセージを残す](#))

Explanation/Reference:

The NOT keyword is used in this question. You need to find out an option which is not true about job scheduling.

以下に、ジョブスケジューリング、またはジョブスケジューリングソフトウェアを使用する利点をいくつか示します。

ジョブ情報は一度設定するだけで済むため、エラーの可能性が低減されます。

すべての仕事の成功と失敗に関する記録が保管されている。

通信事業者への依存度が低下する。

ジョブの依存関係は、あるジョブが失敗した場合、そのジョブの出力に依存する後続のジョブが処理されないように定義されています。

試験を受けるにあたっては、以下の情報を知っておく必要があります。

ジョブスケジューラとは、無人でバックグラウンドで実行されるプログラム（一般にバッチ処理と呼ばれる）を制御するためのコンピュータアプリケーションである。

同義語としては、バッチシステム、分散リソース管理システム（DRMS）、分散リソースマネージャ（DRM）などがあります。今日のジョブスケジューラは、ワークロード自動化と呼ばれることが多く、通常、グラフィカルユーザーインターフェイスと、分散コン

コンピュータネットワークにおけるバックグラウンド実行の定義と監視のための単一の制御ポイントを提供します。ジョブスケジューラには、さまざまなオペレーティングシステムプラットフォームやビジネスアプリケーション環境にわたって、リアルタイムのビジネス活動と従来のバックグラウンドIT処理の統合を調整することがますます求められています。

ジョブスケジューリングは、プロセススケジューリングと混同してはならない。プロセススケジューリングとは、オペレーティングシステムが現在実行中のプロセスをCPUに割り当てることである。

ジョブスケジューラソフトウェアに求められる基本的な機能は以下のとおりです。

ワークフローやジョブの依存関係を定義するのに役立つインターフェース

執行の自動送信

実行を監視するためのインターフェース

優先順位やキューを使用して、関連性のないジョブの実行順序を制御する。全く異なる分野のソフトウェアがこれらの機能のすべてまたは一部を含んでいる場合、そのソフトウェアはジョブスケジューリング機能を備えているとみなされる。

ほとんどのオペレーティングシステム（UnixやWindowsなど）は、cronなどの基本的なジョブスケジューリング機能を提供しています。Webホスティングサービスも、コントロールパネルやwebcronソリューションを通じてジョブスケジューリング機能を提供しています。DBMS、バックアップ、ERP、BPMなどの多くのプログラムにも、関連するジョブスケジューリング機能が含まれています。オペレーティングシステム（OS）または特定のプログラムが提供するジョブスケジューリング機能は、通常、単一のOSインスタンスを超えて、または特定のプログラムの範囲外でのスケジューリング機能を提供しません。

関連性のないITワークロードを自動化する必要がある組織は、ジョブスケジューラのさらに高度な機能を活用することもできます。例えば、次のような機能です。

外部の予測不可能なイベントに基づくリアルタイムスケジューリング

障害発生時の自動再起動と復旧

運用担当者への警告および通知

インシデントレポートの生成

規制遵守目的の監査証跡

以下の回答は誤りです。

その他のオプションは、ジョブスケジューリングに関して正しく定義されています。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版、242ページ

http://en.wikipedia.org/wiki/Job_scheduler

最新問題: 625

Which of the following criteria is MOST important for the successful delivery of benefits from an IT project?

- A. Assessing the impact of changes to individuals and business units within the organization
- B. Ensuring that IT project managers have sign-off authority on the business case
- C. Involving key stakeholders during the development and execution phases of the project
- D. Quantifying the size of the software development effort required by the project

Answer: C ([メッセージを残す](#))

最新問題: 626

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- A. control self-assessments.

- B. a business impact analysis.
- C. an IT balanced scorecard.
- D. business process reengineering.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. Control self-assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

最新問題: 627

An IS auditor needs to validate business logic execution by tracing through production logs.

Which of the following are MOST likely to contain the appropriate entries?

- A. Print server logs
- B. Database logs
- C. File server logs
- D. Application logs

Answer: D ([メッセージを残す](#))

Application logs are most likely to contain entries related to business logic execution, as they record events and transactions specific to the application's operations, including user actions, process flows, and system interactions that implement business logic.

最新問題: 628

請求書の合計請求金額は、毎週自動的に組織の会計帳簿に転送されます。

IS監査の過程で、監査担当者は元帳から1週間分の請求データが欠落していることを発見しました。監査担当者は、以下のどの領域を最初に調査すべきでしょうか？

- A. 年間調整
- B. 変更管理
- C. バッチ処理制御
- D. モジュールアクセス権限

Answer: C ([メッセージを残す](#))

セクション：情報システムの監査プロセス

最新問題: 629

IS監査担当者は、IS管理部門から、組織が最近ソフトウェア能力成熟度モデル（CMM）の最高レベルに達したと伝えられた。組織が最近追加したソフトウェア品質プロセスは次のうちどれか。

- A. 継続的な改善。
- B. 定量的な品質目標。
- C. 文書化されたプロセス。

D. 特定のプロジェクトに合わせて調整されたプロセス。

Answer: A ([メッセージを残す](#))

組織は、ソフトウェアCMMの最高レベルであるレベル5（最適化に到達していることになります。定量的な品質目標はレベル4以下で達成可能であり、文書化されたプロセスはレベル3以下で実行可能であり、特定のプロジェクトに合わせたプロセスはレベル3以下で実現可能です。

最新問題: 630

A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

- A. Full-scale test with relocation of all departments, including IT, to the contingency site
- B. Walk-through test of a series of predefined scenarios with all critical personnel involved
- C. IT disaster recovery test with business departments involved in testing the critical applications
- D. Functional test of a scenario with limited IT involvement

Answer: D ([メッセージを残す](#))

机上演習の実施後、次のステップは機能テストであり、これには復旧の管理機能と組織機能を訓練するためのスタッフの動員が含まれます。復旧のIT部分は何年もテストされているため、本格的なテストにITを実際に参加させる前に、事業継続計画（BCP）を検証および最適化する方が効率的です。本格的なテストは、通常の年間テストスケジュールに入る前の検証プロセスの最終ステップです。説明されている状況での本格的なテストは、計画が実際に実行されるのは初めてであるため、失敗する可能性があります。多くのリソース（ITを含む）と時間が無駄になります。ウォークスルーテストは最も基本的なタイプのテストです。その目的は、計画の適切性を検証するのではなく、主要なスタッフに計画を熟知させ、重要な計画要素について議論することです。アプリケーションの復旧は、純粋にIT主導ではなく、常にビジネスによって検証および承認されるべきです。災害復旧テストは、ITに関係のないBCPの管理部分と組織部分を検証するのに役立ちません。

トピック8、複合質問

最新問題: 631

小規模組織において、情報システム監査担当者が、セキュリティ管理とシステム分析の機能を同一従業員が担当していることを発見しました。以下のうち、最も重要な発見はどれですか？

- A. 従業員の正式な職務記述書が更新されていません。
- B. 従業員の活動は独立した審査を受けていません。
- C. セキュリティポリシーは現状を反映して更新されていません。
- D. 従業員がセキュリティポリシーに署名していません。

Answer: B ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 632

IS監査担当者は、アクセス権限が定期的に見直されたり更新されたりしていないことを知りました。トランザクションが権限のある従業員によって実行されたかどうかを判断するための最良の証拠となるのは、次のうちどれでしょうか？

- A. 監査証跡
- B. 管理合計
- C. 和解
- D. 変更履歴

Answer: A ([メッセージを残す](#))

取引が承認された従業員によって実行されたかどうかを判断する最良の証拠は、監査証跡です。監査証跡は、イベントや手順を記録してサポート文書を提供する安全な記録です。これらは、セキュリティおよび運用上のアクションを認証したり、課題を軽減したり、コンプライアンスと運用上の整合性の証明を提供したりするために使用されます²。監査証跡は、取引に関連する次の情報を追跡およびトレースできます。

- * 取引を開始、承認、変更、または削除した人物
- * 取引が発生した日時
- * 取引が行われた場所（場所またはデバイス）
- * どのような種類の取引（アクションまたは操作）が実行されましたか？
- * 取引が実行された理由（目的または理由）

監査証跡を分析することで、情報システム監査担当者は、取引が権限のある従業員によって実行されたかどうかを確認できます。監査証跡は、発生した可能性のある不正な取引、詐欺的な取引、または誤った取引を特定することもできます。また、監査証跡は、取引から生じる可能性のある紛争や不一致を解決するのに役立ちます。

参考文献：

- * 監査証跡とは？知っておくべきことすべて

最新問題: 633

ある企業は、生産計画におけるすべての変更を文書化し承認するために標準様式を使用しています。これらの様式が適切に承認されていることを確認するために、次のうち最も効果的なサンプリング方法はどれですか？

- A. 発見
- B. 可変
- C. 属性
- D. 金銭

Answer: A ([メッセージを残す](#))

最新問題: 634

次の機密性、完全性、可用性（CIA）属性のうち、情報へのアクセスを許可された意図されたユーザーのみに提供することで最小権限の原則をサポートするものはどれですか？

- A. 機密保持
- B. 誠実さ

C. 入手可能性

D. 精度

Answer: A ([メッセージを残す](#))

説明／参考資料：

機密保持は、最小権限の原則」を支えるものであり、情報へのアクセスは、必要最小限の範囲で、権限を与えられた個人、プロセス、またはシステムのみ限定されるべきであるという原則に基づいています。

権限を与えられた個人が持つべきアクセスレベルは、その職務を遂行するために必要なレベルであるべきです。近年、情報のプライバシーと、情報を閲覧することで犯罪を犯す可能性のある個人から情報を保護する必要性について、多くの報道がなされています。

なりすましとは、様々な情報源から入手した機密情報を利用して、他人の身元を偽る行為のことである。

情報の機密性を確保するための重要な対策の一つは、データの分類です。これは、誰が情報にアクセスできるか（公開 内部利用のみ、機密）を判断するのに役立ちます。アクセス制御による識別、認証、認可は、情報の機密性を維持する上で有効な手段です。機密性を保護するための対策の一つとして、情報の暗号化が挙げられます。情報を暗号化することで、権限のない人物が情報にアクセスした場合でも、その情報の利用可能性を制限できます。

試験を受けるにあたっては、以下の情報を知っておく必要があります。

誠実さ

情報の完全性とは、意図的、無許可、または偶発的な変更から情報を保護すべきであるという原則である。

ファイル、データベース、システム、ネットワークに保存されている情報は、取引を正確に処理し、ビジネス上の意思決定に必要な正確な情報を提供するために不可欠です。そのため、情報が適切な方法で変更されることを保証するための管理体制が整備されています。

管理上の対策としては、職務分掌、システム開発ライフサイクルにおける承認チェックポイント、情報整合性の確保に役立つテスト手法の導入などが挙げられます。適切に構成されたトランザクションと更新プログラムのセキュリティは、システムへの変更適用において一貫性のある方法を提供します。更新へのアクセスを、アクセスが必要な担当者のみ限定することで、意図的および非意図的な変更のリスクを軽減できます。

可用性

可用性とは、必要なときにユーザーが情報にアクセスできることを保証する原則である。

システムの可用性に影響を与える主な要因は次の2つです。

1. サービス拒否攻撃と

2. 人為的な災害（例：容量計画不備によるシステムクラッシュ、旧式のハードウェア、アップグレード後のテストの不備によるシステムクラッシュ）または自然災害（例：地震、竜巻、停電、ハリケーン、火災、洪水）によるサービスの中断。

いずれの場合も、エンドユーザーは業務遂行に必要な情報にアクセスできません。システムの重要性和組織の存続におけるその重要性によって、システム停止期間が長引いた場合の影響の深刻さが決まります。適切なセキュリティ対策が講じられていないと、ウイルス感染、データ破壊、外部からの侵入、サービス拒否（DoS）攻撃などのリスクが高まります。

このような事態が発生すると、通常のユーザーによるシステムの使用が妨げられる可能性があります。

CIA

以下の回答は誤りです。

完全性 — 完全性とは、情報が意図的、不正、または偶発的な変更から保護されるべきであるという原則である。

可用性 — 可用性とは、必要なときにユーザーが情報にアクセスできることを保証する原則です。

正確性 - 正確性はCIAの有効な属性ではありません。



この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 314ページ

ISC2公式CISSP CBKガイド第3版 350ページ

最新問題: 635

システムソフトウェアとデータを保護する上で、一般的に最も重視される対策は何ですか？

- A. 管理アクセス制御
- B. 論理アクセス制御
- C. 物理的なアクセス制御
- D. 探偵アクセス制御

Answer: ([解答を表示する](#))

論理アクセス制御は、システムソフトウェアとデータの主要な保護策となることが多い。

最新問題: 636

以下のうち、最高セキュリティ責任者（CSO）の通常の実任範囲はどれですか？

- A. セキュリティポリシーを定期的に見直し、評価する
- B. ユーザーアプリケーションおよびソフトウェアのテストと評価の実施
- C. ITリソースへのユーザーアクセス権の付与と取り消し
- D. データおよびアプリケーションへのアクセス承認

Answer: ([解答を表示する](#))

最高セキュリティ責任者（CSO）の役割は、企業セキュリティポリシーと管理体制が、データ、プログラム、機器などの企業資産への不正アクセスを防止するのに十分であることを保証することです。ユーザーアプリケーションやその他のソフトウェアのテストと評価は、通常、開発および保守を担当するスタッフの責任です。ITリソースへのアクセス権の付与と取り消しは、通常、ネットワーク管理者またはデータベース管理者の業務です。データおよびアプリケーションへのアクセス承認は、データ所有者の責務です。

最新問題: 637

The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

- A. achieve performance improvement.
- B. provide user authentication.
- C. ensure availability of data.
- D. ensure the confidentiality of data.

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

最新問題: 638

新しい財務アプリケーションの開発において、IS監査人が最初に関与すべき事項は以下のとおりです。

- A. 制御設計。
- B. 実現可能性調査。
- C. アプリケーション設計。
- D. システムテスト。

Answer: B ([メッセージを残す](#))

新しい財務アプリケーションの開発において、IS監査担当者が最初に関与すべきは、実現可能性調査です。実現可能性調査とは、提案されたプロジェクトまたはシステムの技術的、運用的、経済的、および法的側面を評価する予備的な分析です。実現可能性調査は、プロジェクトまたはシステムが組織とその利害関係者にとって実行可能で、実現可能で、望ましいものであるかどうかを判断するのに役立ちます。

IS監査担当者の役割は、実現可能性調査において、プロジェクトまたはシステムのリスク、メリット、コスト、および影響について、独立した客観的な評価を提供することです。IS監査担当者は、実現可能性調査が構造化された体系的なアプローチに従い、関連するすべての要因と代替案を考慮し、組織の方針と基準に準拠していることを確認する必要があります。また、IS監査担当者は、実現可能性調査が文書化され、適切な意思決定者に伝達されていることを確認する必要があります。

IS監査担当者が実現可能性調査に関与することは、以下のような点で重要です。

プロジェクトまたはシステムの成功に影響を与える可能性のある潜在的なリスクと問題を特定し、軽減する。

プロジェクトまたはシステムが組織の戦略、目標、および価値提案と整合しているかどうかを評価し、正当化する。

プロジェクトまたはシステムの資源、予算、スケジュール、品質を見積もり、最適化する

プロジェクトまたはシステムのセキュリティ、信頼性、パフォーマンス、ユーザビリティを評価し、向上させる。

* プロジェクトまたはシステムが、ユーザーおよびその他の利害関係者の期待と要件を満たしていることを確認します。他の3つのオプションは、新しい財務アプリケーションの開発におけるIS監査人の最初に関与ではありませんが、開発プロセスの次の段階の一部となる可能性があります。コントロール設計は、システムのセキュリティ、完全性、可用性、および効率性を保証するコントロールを定義して実装するプロセスです。アプリケーション設計は、システムの機能的および技術的な特徴を指定するプロセスです。システムテストは、システムが仕様と要件を満たしていることを検証するプロセスです。

したがって、実現可能性調査が最善の解決策である。

参考文献：

* [実現可能性調査 - ISACA]

* [IS監査ガイドラインG13 IS監査業務の実施 - ISACA]

最新問題: 639

次のハニーポットのうち、ハッカーに攻撃のための実際の環境を提供するものはどれですか？

- A. 高相互作用

- B. 低相互作用
- C. 薬物相互作用
- D. 選択肢に該当するものではありません

Answer: ([解答を表示する](#))

セクション：情報資産の保護

Explanation:

高インタラクショナル型のハニーポットは、攻撃者に攻撃を行うための現実的な環境を提供するという点で共通している。

また、CISA試験のハニーポットに関する以下の情報も知っておく必要があります。

ハニーポットとは、インターネット上の不運なサーバーを装うソフトウェアアプリケーションであり、侵入に対する積極的な防御機能は設定されていない。

ハニーポットには2種類あります。

高インタラクショナル型ハニーポットは、ハッカーに攻撃のためのリアルな環境を提供します。高インタラクショナル型ハニーポットは、様々なサービスをホストする本番システムの活動を模倣するため、攻撃者は多くのサービスにアクセスして時間を浪費することができます。高インタラクショナル型ハニーポット技術に関する最近の研究によると、仮想マシンを使用することで、1台の物理マシン上に複数のハニーポットをホストすることが可能です。そのため、ハニーポットが侵害された場合でも、より迅速に復旧できます。

一般的に、インタラクショナル頻度の高いハニーポットは検出が困難なためセキュリティが向上しますが、維持管理コストが非常に高くなります。仮想マシンが利用できない場合は、物理コンピュータごとに1つのハニーポットを維持する必要があり、これは非常に高額になる可能性があります。例：ハニーネット。

低インタラクショナル - 本番環境をエミュレートするため、提供する情報はより限定的です。低インタラクショナルのハニーポットは、攻撃者が頻繁に要求するサービスのみをシミュレートします。リソース消費量が比較的少ないため、1台の物理システム上で複数の仮想マシンを容易にホストでき、仮想システムの応答時間が短く、必要なコードも少ないため、仮想システムのセキュリティの複雑さが軽減されます。例：Honeyed。

以下の回答は誤りでした。

薬物相互作用 - 本物のハニーポットではありません

参照：

CISAレビューマニュアル2014年版 348ページ

http://en.wikipedia.org/wiki/Honeypot_%28computing%29

http://www.ce-infosys.com/english/free_compusec/free_compusec.aspx

最新問題: 640

Which of the following virus prevention techniques can be implemented through hardware?

- A. Remote booting
- B. Heuristic scanners
- C. Behavior blockers
- D. Immunizers

Answer: ([解答を表示する](#))

Section: Protection of Information Assets

Explanation:

Remote booting (e.g., diskless workstations) is a method of preventing viruses, and can be implemented

through hardware. Choice C is a detection, not a prevention, although it is hardware-based. Choices B and D are not hardware-based.

最新問題: 641

Which of the following types of spyware was originally designed for determining the sources of error or for measuring staff productivity?

- A. Keywords logging
- B. Keystroke logging
- C. Directory logging
- D. Password logging
- E. None of the choices.

Answer: B ([メッセージを残す](#))

Keystroke logging (in the form of spyware) was originally a function of diagnostic tool deployed by software developers for capturing user's keystrokes.

This is done for determining the sources of error or for measuring staff productivity.

最新問題: 642

ユーザーがシステムレベルでデータベースに直接アクセスできる場合、リスクはどのように影響を受けるのでしょうか？

- A. 不正アクセスのリスクは増加するが、データベースへの追跡不可能な変更のリスクは減少する。
- B. データベースへの不正かつ追跡不可能な変更のリスクが増大します。
- C. 不正アクセスのリスクは減少しますが、データベースへの追跡不可能な変更のリスクは増加します。
- D. データベースへの不正な変更や追跡不可能な変更のリスクが低減します。

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

ユーザーがシステムレベルでデータベースに直接アクセスできる場合、データベースへの不正な変更や追跡不可能な変更のリスクが高まります。

最新問題: 643

An IS auditor is assigned to perform a post-implementation review of an application system.

Which of the following would impair the auditor's independence?

- A. The auditor designed an embedded audit module exclusively for audit.
- B. The auditor implemented a specific control during the development of the system.
- C. The auditor participated as a member of the project team without operational responsibilities.
- D. The auditor provided advice concerning best practices.

Answer: B ([メッセージを残す](#))

最新問題: 644

Which of the following activities should occur after a business impact analysis (BIA)?

- A. Identify critical applications

- B. Analyze recovery options
- C. Review the computing and user environment
- D. Identify threats to the IT environment

Answer: A ([メッセージを残す](#))

最新問題: 645

大規模アプリケーション開発プロジェクトにおける統制の評価において、IS監査担当者の時間を最も効果的に活用する方法は、以下の項目をレビューおよび評価することである。

- A. 費用便益分析。
- B. プロジェクト計画。
- C. 受け入れテスト
- D. アプリケーションのテストケース。

Answer: D ([メッセージを残す](#))

最新問題: 646

以下のうち、内部監査機能の役割を明確に示しているのはどれですか？

- A. 監査ガバナンス
- B. 監査憲章
- C. 監査目的
- D. 監査プロジェクト計画

Answer: ([解答を表示する](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 647

インシデント対応計画の主な目的は以下のとおりです。

- A. 情報資産に対する有害事象の影響を軽減する。
- B. 予防的管理の効果を高める。
- C. 影響を受けるシステムの最大許容ダウンタイム (MTD)を削減する。
- D. ITシステムに対する有害事象の影響についての認識を高める。

Answer: ([解答を表示する](#))

インシデント対応計画の主な目的は、情報資産に対する有害事象の影響を軽減することです。インシデント対応計画とは、セキュリティ侵害、サイバー攻撃、または情報システムやデータに影響を与えるその他の障害が発生した場合に、組織が取るべき行動を規定する一連の指示と手順のことです。

インシデント対応計画の目的は以下のとおりです。

事件をできるだけ早く検知し、特定する。

さらなる被害や拡散を防ぐため、事件を封じ込め、隔離する。

事件の原因、規模、影響を判断するために、事件を分析 調査する。

影響を受けたシステムとデータから、インシデントとその根本原因を根絶 排除する。

システムとデータの正常な動作と機能を復旧 復元する。

今回の事案から得られた教訓、ベストプラクティス、そして将来の予防と軽減のための提言を文書化することで、学びと改善を図りましょう。

インシデント対応計画に従うことで、組織は情報資産に対する有害事象の悪影響を最小限に抑えることができます。例えば、以下のような影響が挙げられます。

データまたは情報の損失または破損。

機密情報または機密性の高いデータもしくは情報の漏洩または盗難。

システムまたはサービスの可用性もしくはパフォーマンスの中断または低下。

法令違反または規制違反、あるいは法的責任。

金銭的損失または評判の損失もしくは損害。

インシデント対応計画は、組織が情報資産を保護し、法的および契約上の義務を遵守する上で、適切な注意義務と説明責任を果たしていることを示す上でも役立ちます。

その他の選択肢は、インシデント対応計画の主要な目的ではありませんが、計画を策定することによる副次的な利点や成果となる可能性があります。

予防措置の有効性を高めることは、インシデント対応計画の主要な目的ではない。

予防的制御とは、ファイアウォール、ウイルス対策ソフトウェア、暗号化、認証など、そもそも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です。インシデント対応計画は、インシデントが発生した後に対処する事後的な制御です。しかし、インシデント対応計画は、予防的制御の弱点や欠陥を特定して対処することで、予防的制御の有効性を向上させるのに役立つ場合があります。

インシデント対応計画の主な目的は、影響を受けるシステムの最大許容ダウンタイム (MTD) を短縮することではありません。MTDとは、組織がシステムやサービスの停止によって事業運営や目標に許容できない損害や損失が生じる前に、どれだけの時間までシステムやサービスの停止を許容できるかを示す指標です。インシデント対応計画は、より迅速かつ円滑な復旧プロセスを促進することで、影響を受けるシステムのMTDを短縮するのに役立つ可能性があります。

しかし、MTD（最大治療日数を削減することは、インシデント対応計画の主要な目標ではなく、望ましい結果の一つに過ぎない。インシデント対応計画の主な目的は、ITシステムへの有害事象の影響に対する認識を高めることではありません。認識とは、何かについて情報を得たり、意識したりする状態のことです。インシデント対応計画は、経営陣、従業員、顧客、規制当局などの関係者に情報やコミュニケーションチャネルを提供することで、ITシステムへの有害事象の影響に対する認識を高めるのに役立つ可能性があります。

しかし、意識向上はインシデント対応計画の主な目的ではなく、むしろ影響の軽減、法令遵守の確保、信頼の維持といった他の目的を達成するための手段である。

最新問題: 648

Which of the following stakeholders is accountable for control evaluations during a control self-assessment (CSA)?

A. Enterprise risk management

B. Quality assurance management

C. Departmental managers

D. Chief internal auditor

Answer: B ([メッセージを残す](#))

最新問題: 649

以下のどの制御が、入力データが事前に定義された基準に準拠していることを保証しますか？

可能な値のコンピュータ化された表？

A. 範囲チェック

B. テーブル参照

C. 存在チェック

D. 妥当性チェック

Answer: B ([メッセージを残す](#))

セクション：情報システムの取得、開発、導入

説明

説明／参考資料：

テーブル検索では、入力データはコンピュータ化されたテーブルに保持されている事前定義された基準に準拠します。値。たとえば、入力チェックでは、1から10までの都市コードを入力します。この番号は、コードと都市名を対応付ける表をコンピュータ化する。

CISA試験では、以下のデータ検証の編集と制御について理解しておく必要があります。

シーケンスチェック - 管理番号は順番に続きます。シーケンスまたは重複した管理番号は

numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check - Data should not exceed a predefined amount. For example, payroll checks should not exceed US \$ 4000. If a check exceeds US \$ 4000, data would be rejected for further verification/ authorization.

Validity Check - Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or

S. If any other

code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check - Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups - Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check - Data are entered correctly and agree with valid predefined criteria. For example, a valid

transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit - a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check - a field should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. This is identified as a key in field and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already

入力されました。例: ベンダー請求書番号が以前に記録された請求書と一致し、
今回の注文は重複注文ではないため、ベンダーに二重に支払いが行われることはありません。

論理関係チェック - 特定の条件が真である場合、1 つ以上の追加条件またはデータ

入力関係は真である必要があり、入力が有効であるとみなされる場合があります。例：

従業員は、入力内容を真実かつ有効なものとして扱うことが求められる場合があります。例：従業員の入社日
生年月日から16年以上経過していることが求められる場合がある。

以下の回答は誤りでした。

範囲チェック - データは、事前に定義された値の範囲を超えてはなりません。例：製品タイプコード
範囲は100から250です。この範囲外のコードは、無効な製品タイプとして拒否されます。

存在チェック - データが正しく入力され、有効な事前定義基準に合致している。たとえば、有効な
取引コードは、取引コード欄に入力する必要があります。

妥当性チェック - 入力データは、事前に定義された妥当な制限または発生率と照合されます。

例えば、ウィジェットメーカーは通常、20個以下のウィジェットの注文を受けます。

20個を超えるウィジェットが受信された場合、コンピュータプログラムは警告とともに記録を出力するように設計する必要があります。

その命令は不当であると思われることを示している。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 215ページ

最新問題: 650

エンドユーザーコンピューティング (EUC)において、財務報告にスプレッドシートを利用することに伴う最大のリスクは次のうちどれですか？

- A. 運用上のインシデントの増加
- B. 規制違反の増加
- C. パスワード保護の欠如
- D. 処理の完全性の欠如

Answer: D ([メッセージを残す](#))

最新問題: 651

次の記述のうち、デバイスとそのTCP/IPモデル内での位置づけを誤って説明しているのはどれですか？

- A. レイヤー4スイッチはTCP/IPモデルのネットワークインターフェース層で動作します。
- B. ルーターはTCP/IPモデルのネットワークインターフェース層で動作します。
- C. レイヤー3スイッチはTCP/IPモデルのネットワークインターフェース層で動作します。
- D. ハブはTCP/IPモデルのLANまたはWANインターフェース層で動作します

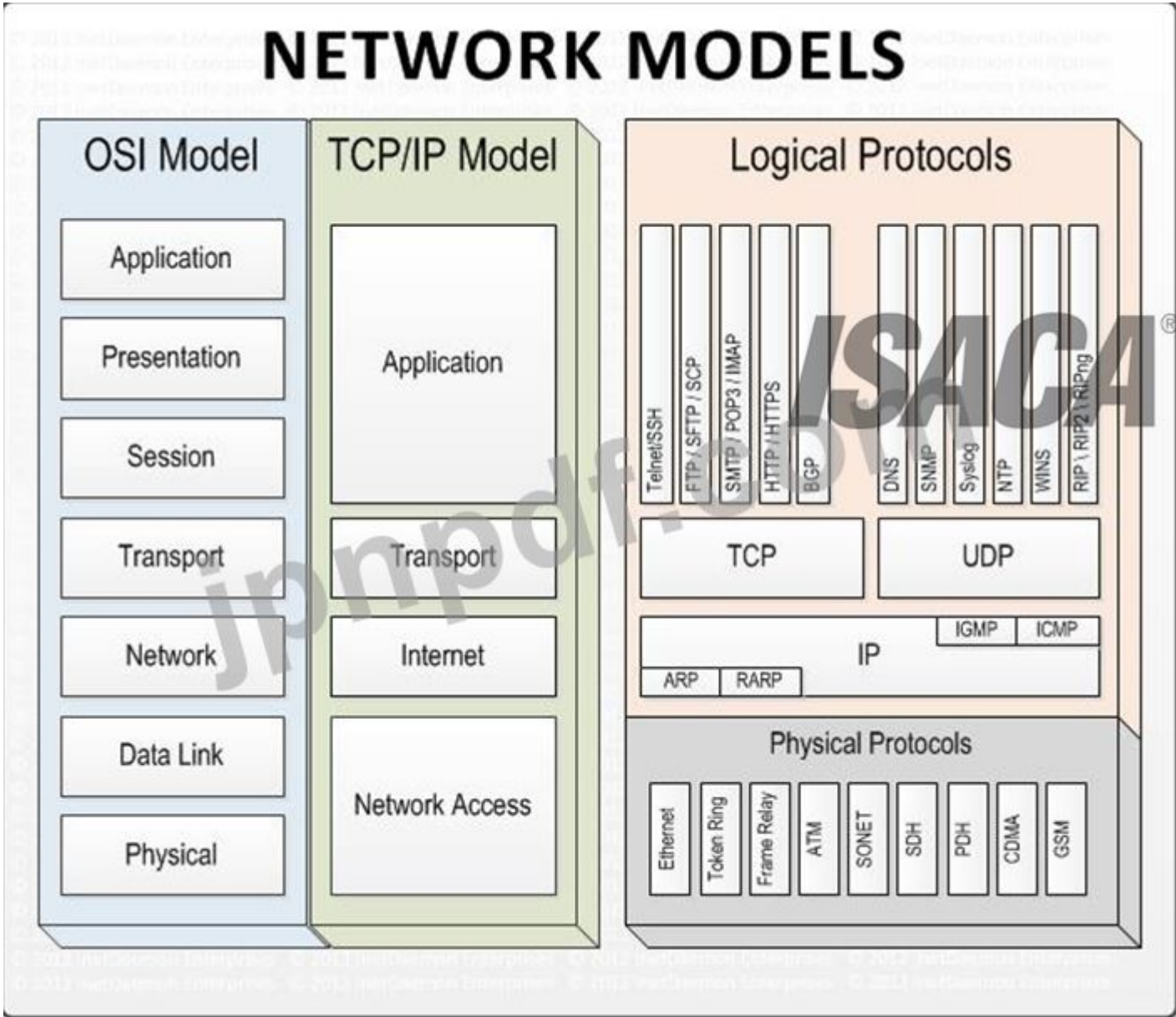
Answer: ([解答を表示する](#))

説明／参考資料：

質問のキーワードは「誤って」です。誤っている記述を見つける必要があります。

試験に向けて、TCP/IPモデルに関する以下の情報を知っておく必要があります。

ネットワークモデル



第4層 :アプリケーション層

アプリケーション層は、4層構造のTCP/IPモデルにおいて最上位の層です。アプリケーション層はトランスポート層の上に位置します。アプリケーション層は、TCP/IPアプリケーションプロトコルと、ホストプログラムがネットワークを利用するためにトランスポート層サービスとどのように連携するかを定義します。

アプリケーション層には、DNS（ドメイン命名システム）、HTTP（ハイパーテキスト転送プロトコル）、Telnet、SSH、FTP（ファイル転送プロトコル）、TFTP（簡易ファイル転送プロトコル）、SNMP（簡易ネットワーク管理プロトコル）、SMTP（簡易メール転送プロトコル）、DHCP（動的ホスト構成プロトコル）、X Window、RDP（リモートデスクトッププロトコル）など、上位レベルのプロトコルがすべて含まれます。

レイヤー3. トランスポート層

トランスポート層は、4層構造のTCP/IPモデルにおける第3層です。トランスポート層は、アプリケーション層とインターネット層の間に位置します。トランスポート層の目的は、送信元ホストと宛先ホスト上のデバイスが通信を行えるようにすることです。トランスポート層は、データ転送時に使用される接続のサービスレベルと状態を定義します。

トランスポート層に含まれる主なプロトコルは、TCP（伝送制御プロトコル）とUDP（ユーザーデータグラムプロトコル）です。

レイヤー2. インターネット層

インターネット層は、4層構造のTCP/IPモデルにおける第2層です。インターネット層は、ネットワークアクセス層とトランスポート層の間に位置します。インターネット層は、IPデータグラムと呼ばれるデータパケットにデータを圧縮します。IPデータグラムには、送信元アドレスと宛先アドレス（論理アドレスまたはIPアドレス）の情報が含まれており、ホスト間およびネットワーク間でデータグラムを転送するために使用されます。インターネット層は、IPデータグラムのルーティングも担当します。

パケット交換ネットワークは、コネクションレス型のインターネットワーク層に依存しています。この層はインターネット層と呼ばれ、ホストが任意のネットワークにパケットを挿入し、宛先まで独立して配信できるようにする役割を担っています。宛先側では、データパケットは送信時とは異なる順序で到着する場合があります。上位層は、これらのパケットを適切なネットワークアプリケーション（アプリケーション層で動作）に配信するために、順序を並べ替える役割を担います。

インターネット層に含まれる主なプロトコルは、IP（インターネットプロトコル）、ICMP（インターネット制御メッセージプロトコル）、ARP（アドレス解決プロトコル）、RARP（逆アドレス解決プロトコル）、およびIGMP（インターネットグループ管理プロトコル）です。

レイヤー1. ネットワークアクセスレイヤー

ネットワークアクセス層は、4層構造のTCP/IPモデルの最初の層です。ネットワークアクセス層は、データがネットワークを介して物理的に送信される方法の詳細を定義します。これには、同軸ケーブル、光ファイバー、ツイストペア銅線などのネットワーク媒体と直接接続するハードウェアデバイスによって、ビットが電氣的または光学的にどのように信号化されるかが含まれます。ネットワークアクセス層に含まれるプロトコルには、イーサネット、トークンリング、FDDI、X.25、フレームリレーなどがあります。

上記に挙げたLANアーキテクチャの中で最も一般的なのはイーサネットです。イーサネットは、共有メディアで動作する場合、CSMA/CD（キャリアセンス多重アクセス/衝突検出）と呼ばれるアクセス方式を使用してメディアにアクセスします。アクセス方式は、ホストがメディア上にデータを配置する方法を決定します。

CSMA/CDアクセス方式では、すべてのホストが媒体に平等にアクセスでき、ネットワークトラフィックがないときにデータを送信できます。ホストがデータを送信しようとする、他のホストが既に媒体を使用しているかどうかを確認します。媒体にトラフィックがある場合は、ホストは待機し、トラフィックがない場合は、データを媒体に送信します。しかし、2つのシステムが同時に媒体にデータを送信しようとする、衝突が発生し、データが破壊されます。送信中にデータが破壊された場合は、データを再送信する必要があります。衝突後、各ホストは短い時間待機し、その後、データが再送信されます。

プロトコルデータユニット（PDU）：



プロトコルデータユニット - PDU

以下の回答は誤りです。

他の選択肢は、TCP/IPモデルに基づいたネットワークデバイスの動作について正しく説明しています。この問題を作成するために、以下の資料が使用されました。

CISAレビューマニュアル2014年版、272ページ

最新問題: 652

分析テストにデータを利用する前に、まず最初に行うべきことはどれですか？

- A. データ分析テストスクリプトを検証する。
- B. データ取得に使用した抽出ツールを文書化する。
- C. 分析サンプリングおよびテストモデルを選択します。
- D. データの完全性と正確性を確認する。

Answer: D ([メッセージを残す](#))

最新問題: 653

Which of the following should be GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

- A. Data conversion was performed using manual processes.
- B. Backups of the old system and data are not available online.
- C. Unauthorized data modifications occurred during conversion.
- D. The change management process was not formally documented

Answer: (解答を表示する)

The greatest concern for an IS auditor reviewing data conversion and migration during the implementation of a new application system is unauthorized data modifications occurred during conversion. Unauthorized data modifications are changes or alterations to data that are not authorized, intended, or expected, such as due to errors, fraud, or sabotage. Unauthorized data modifications occurred during conversion can compromise the accuracy, completeness, and integrity of the data being converted and migrated to the new application system, and may result in data loss, corruption, or inconsistency. The other options are not as concerning as unauthorized data modifications occurred during conversion in reviewing data conversion and migration during the implementation of a new application system, as they do not affect the accuracy, completeness, or integrity of the data being converted and migrated. Data conversion was performed using manual processes is a possible factor that may increase the risk or complexity of data conversion and migration, but it does not necessarily imply that unauthorized data modifications occurred during conversion. Backups of the old system and data are not available online is a possible factor that may affect the availability or accessibility of the old system and data for backup or recovery purposes, but it does not imply that unauthorized data modifications occurred during conversion. The change management process was not formally documented is a possible factor that may affect the quality or consistency of the change management process for implementing the new application system, but it does not imply that unauthorized data modifications occurred during conversion.

References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

最新問題: 654

あるグローバル企業が所在する国で、個人データの国境を越えた移転を禁止する新たな規制が最近施行されました。情報システム監査担当者は、当該国における組織のセキュリティリスクレベルを判断するよう依頼されました。この評価を行う上で、次のうちどれが最も役立つでしょうか？

- A. 影響を受ける管轄区域と個人データを交換するすべての事業体の目録を作成する
- B. 影響を受ける管轄区域におけるデータセキュリティ脅威の特定
- C. 影響を受ける管轄区域に関連するデータ分類手順の見直し
- D. 影響を受ける管轄区域との個人データ交換に関連する業務プロセスを特定する

Answer: D (メッセージを残す)

影響を受ける管轄区域との間で個人データのやり取りを行う業務プロセスを特定することは、影響を受ける国における組織の情報漏洩リスクのレベルを評価する上で最も有効な活動です。

IS監査担当者は、組織の事業運営と機能が個人データの国境を越えた移転にどのように依存しているか、あるいは関わっているか、また、新たな規制が事業継続性とコンプライアンスに及ぼす潜在的な影響とリスクを理解しておく必要があります。その他の選択肢は、評価のための追加情報や背景情報を提供する可能性はあるものの、評価の主要な焦点ではないため、あまり役に立たない活動です。参考文献：

* CISAレビューマニュアル (デジタル版)、第7章、7.4.21節

* CISA復習問題、解答、解説データベース、問題ID 221

最新問題: 655

ファイアウォールポリシーを作成する際の最初のステップはどれですか？

- A. アプリケーションのセキュリティを確保するための方法の費用対効果分析
- B. 外部からアクセスするネットワークアプリケーションの識別
- C. 外部からアクセスされるネットワークアプリケーションに関連する脆弱性の特定

D. 保護方法を示すアプリケーショントラフィックマトリックスの作成

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

ネットワーク全体で必要なアプリケーションを最初に特定する必要があります。特定後、ネットワーク内のこれらのアプリケーションの物理的な位置とネットワークモデルに応じて、担当者はこれらのアプリケーションへのアクセスを制御する必要性と可能な方法を理解できます。特定された脆弱性に対する保護方法を特定し、それらの費用対効果分析を行うことが3番目のステップです。アプリケーションを特定したら、次のステップは、ネットワークアプリケーションに関連する脆弱性（弱点を特定することです。次のステップは、アプリケーションのトラフィックを分析し、各タイプのトラフィックがどのように保護されるかを示すマトリックスを作成することです。

最新問題: 656

情報資産が輸送中および廃棄中に適切に保護されているかどうかを判断する際に、最も懸念されるのは次のうちどれですか？

- A. 適切なラベル表示の欠如
- B. 最近の意識向上トレーニングの不足。
- C. パスワード保護の欠如
- D. 適切なデータ分類の欠如

Answer: D ([メッセージを残す](#))

説明

The most concerning issue when determining if information assets are adequately safeguarded during transport and disposal is lack of appropriate data classification. Data classification is a process that assigns categories or levels of sensitivity to different types of information assets based on their value, criticality, or risk to the organization. Data classification can help safeguard information assets during transport and disposal by providing criteria and guidelines for identifying, labeling, handling, and protecting information assets according to their sensitivity. Lack of appropriate data classification can compromise the security and confidentiality of information assets during transport and disposal by exposing them to unauthorized access, disclosure, theft, damage, or destruction. The other options are not as concerning as lack of appropriate data classification in safeguarding information assets during transport and disposal, as they do not affect the identification, labeling, handling, or protection of information assets according to their sensitivity. Lack of appropriate labeling is a possible factor that may increase the risk of misplacing, losing, or mishandling information assets during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. Lack of recent awareness training is a possible factor that may affect the knowledge or behavior of staff involved in transporting or disposing of information assets, but it does not affect the classification of information assets according to their sensitivity. Lack of password protection is a possible factor that may affect the security or confidentiality of information assets stored on devices during transport and disposal, but it does not affect the classification of information assets according to their sensitivity. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

最新問題: 657

ウイルス攻撃を防ぐための最も基本的な手順は次のうちどれですか？

- A. 包括的なウイルス対策ポリシーの策定と周知
- B. ユーザーのデスクトップコンピュータにウイルス対策ソフトウェアを導入する
- C. すべてのネットワーク インターネットゲートウェイでウイルス対策コンテンツチェックを実施する

D. システムにウイルス対策コードを接種する

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

包括的なウイルス対策ポリシーを採用し周知徹底することは、ウイルス感染を防ぐための最も基本的なステップである。ウイルス攻撃。その他のすべてのウイルス対策対策は、以下によって確立され伝達される決定に依存します。ポリシー。

最新問題: 658

Which of the following is the MOST likely reason an organization would use Platform as a Service (PaaS)?

A. To develop and integrate its applications

B. To establish a network and security architecture

C. To operate third-party hosted applications

D. To install and manage operating systems

Answer: A ([メッセージを残す](#))

最新問題: 659

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

A. A sufficient quantity of data for each test case

B. Data representing conditions that are expected in actual processing

C. Completing the test on schedule

D. A random sample of actual data

Answer: B ([メッセージを残す](#))

Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity. It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

最新問題: 660

IS監査担当者が医療施設の物理セキュリティ監査を実施したところ、患者ケアエリアに監視カメラ（CCTV）システムが設置されていることが判明しました。以下のうち、最も懸念されるのはどれですか？

A. カメラは24時間365日監視されているわけではありません。

B. ISの録音が進行中であることを示す通知はありません。

C. ビデオ録画の保存期間は定められていません

D. 動画のバックアップはありません。

Answer: B ([メッセージを残す](#))

患者ケアエリアに設置された監視カメラ（CCTV）システムに関して最も懸念されるのは、録画中であることを示す表示がないことです。これは、医療現場におけるCCTVシステムが、特に個人情報や医療情報が漏洩する可能性のある機密性の高いエリアにおいて、患者、職員、訪問者のプライバシーと機密性を脅かす可能性があるためです。政府の監視カメラ行動規範¹によれば、CCTVオペレーターはCCTVの使用に関して可能な限り透明性を確保し、明確で目立つ標識を用いて録画中であることを人々に知らせ

なければなりません。標識には、CCTVオペレーターの連絡先と監視の目的も記載する必要があります。こうした表示を行うことで、CCTVオペレーターはデータ保護法を遵守し、個人の権利と期待を尊重することができます。

選択肢Bが正解です。録画中であることを示す表示がないことは、地方自治体や警察に適用され、イングランドとウェールズの他のCCTV事業者にも採用が推奨されている監視カメラ行動規範1に明らかに違反しているからです。この規範は、公共空間CCTVに関する国家戦略2とともにスコットランドにも適用されます。この規範は、英国全土に適用される情報コミッショナー事務局(ICO)3が提供するガイダンスと併用することを意図しています。ICOは、CCTV事業者は、CCTV区域の入り口に目立つ標識を設置し、区域内にもさらに標識を設置することで、録画されていることを人々に知らせなければならないと述べています。

選択肢Aは誤りです。カメラが24時間365日監視されていないことは、必ずしも個人のプライバシーや機密性に影響を与えるわけではないため、最大の懸念事項ではありません。CCTVシステムには、犯罪の抑止や監視、セキュリティの強化、患者ケアの向上など、さまざまな目的や目標があります。

用途によっては、CCTVシステムは常時監視ではなく、定期的な点検や分析で十分な場合もあります。しかし、CCTV運用者は、CCTVシステムを不正アクセスや改ざんから保護するための適切なセキュリティ対策を講じる必要があります。

選択肢Cは誤りです。ビデオ録画の保存期間が定められていないことは、個人のプライバシーや機密性に直接影響を与えるものではないため、最大の懸念事項ではありません。しかし、CCTV事業者は、保存ポリシーを明確に定め、文書化し、特定の目的や証拠として必要な場合を除き、必要以上にビデオ録画を保存しないようにする必要があります。保存期間は、明確かつ正当な根拠に基づき、データ保護法および業界ガイドラインに準拠する必要があります。

選択肢Dは誤りです。動画のバックアップがないことは、個人のプライバシーや機密性に影響を与えないため、最大の懸念事項ではありません。しかし、CCTVオペレーターは、特に特定の目的や証拠として動画が必要な場合、バックアップを取ることを検討すべきです。バックアップは、システム障害、災害、悪意のある攻撃によるデータ損失や破損を防ぐのに役立ちます。また、バックアップは不正アクセスや漏洩を防ぐために、安全に保管し、暗号化する必要があります。

最新問題: 661

システム税計算の正確性を証明する最良の方法は以下のとおりです。

- A. 計算プログラムのソースコードの詳細な視覚的レビューと分析
- B. 汎用監査ソフトウェアを使用してプログラムロジックを再構築し、月間合計を計算します。
- C. 処理用のシミュレーション取引を準備し、結果を事前に決定された結果と比較する。
- D. 計算プログラムのソースコードの自動フローチャート作成と分析。

Answer: (解答を表示する)

セクション：情報資産の保護

Explanation:

処理対象となる取引をシミュレーションし、その結果を事前に決定した結果と比較することが、税額計算の正確性を証明する最良の方法です。詳細な視覚的レビュー、フローチャート作成、ソースコードの分析は効果的な方法ではなく、月ごとの合計額では個々の税額計算の正確性を確認することはできません。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 662

データベース管理者の責任範囲は以下のとおりです。

- A. データ所有権の定義。
- B. データ辞書の運用基準を確立する。
- C. 論理データベースと物理データベースの作成。
- D. データの完全性とセキュリティを確保するための基本ルールを確立する。

Answer: C ([メッセージを残す](#))

データベース管理者は、論理データベースと物理データベースの作成および管理を担当します。データの所有権は、組織全体で共有されるデータの場合は、ユーザー部門の責任者または経営陣が決定します。データ辞書の運用基準を確立するのは、情報システム管理部門とデータ管理者の責任です。企業セキュリティポリシーに沿ってデータの整合性とセキュリティを確保するための基本ルールを確立するのは、セキュリティ管理者の役割です。

最新問題: 663

新しい電子商取引システムのデータベース制御をレビューしていた情報システム監査担当者が、データベース構成にセキュリティ上の脆弱性を発見しました。情報システム監査担当者が次に取りべき行動は次のうちどれでしょうか？

- A. 既存の緩和策を特定する。
- B. 調査結果を上級管理職に報告する。
- C. 是正措置の草案作成を支援する。
- D. 弱点を突こうとする。

Answer: (解答を表示する)

IS監査人がデータベース構成にセキュリティ上の脆弱性を発見した場合、次に取りべき行動は、既存の緩和策を特定することです。これには、脆弱性に対処しリスクを軽減するための対策が既の実施されているかどうかを評価することが含まれます。現在の対策状況を理解することで、監査人は問題の深刻度を判断し、追加の是正措置が必要かどうかを判断できます¹。参考文献：

1 <https://www.isaca.org/resources/insights-and-expertise/audit-programs-and-tools>)

最新問題: 664

IS監査担当者が、アジャイルソフトウェア開発手法を採用しているプロジェクトをレビューしています。IS監査担当者は、次のうちどれを発見すると予想すべきでしょうか？

- A. 能力成熟度モデル (CMM) などのプロセスベースの成熟度モデルの使用
- B. タスクレベルの進捗状況をスケジュールに対して定期的に監視する
- C. チームの生産性を最大化するために、ソフトウェア開発ツールを幅広く活用する。
- D. プロジェクトの今後の活用役に役立つ教訓を特定するイテレーション後のレビュー

Answer: D ([メッセージを残す](#))

ソフトウェアプロジェクト管理におけるアジャイルアプローチの重要な原則は、チームの学習と、プロジェクトの進行に合わせてプロジェクト管理とソフトウェア開発プロセスを洗練するためにチームの学習を活用することです。これを実現する最良の方法の1つは、各イテレーションの終わりに、チームがうまくいった点と改善できた点を検討して文書化し、次のイテレーションで実装する改善点を特定することです。CMMとアジャイルは正反対の極に位置します。CMMは、事前に定義された正式なプロセス

と正式なプロジェクト管理およびソフトウェア開発の成果物を重視します。対照的に、アジャイルプロジェクトは、プロジェクトの特定のニーズとチームのダイナミクスに応じてプロセスを洗練することに依存します。さらに、正式な紙ベースの成果物の重要性は低く、チーム内および主要な外部貢献者との効果的な非公式のコミュニケーションが優先されます。アジャイルプロジェクトは、通常4~8週間の短いイテレーションでリリース可能なソフトウェアを作成します。それ自体が、チーム内にかなりのパフォーマンス規律を植え付けます。これに、チームの作業内容の合意と障害の特定を行うための短い毎日のミーティングを組み合わせることで、スケジュールに対するタスクレベルの追跡は不要になります。アジャイルプロジェクトでは適切な開発ツールを使用しますが、ツールは生産性を達成するための主要な手段とは見なされていません。チームの調和、効果的なコミュニケーション、課題を解決する集団的な能力が生産性の鍵となります。

最新問題: 665

Coding standards provide which of the following?

- A. Field naming conventions
- B. Program documentation
- C. Access control tables
- D. Data flow diagrams

Answer: A ([メッセージを残す](#))

最新問題: 666

BYOD (Bring Your Own Device : 私物端末の業務利用)の導入を検討する際、情報セキュリティ管理者にとって最も重要なことは以下の点を確認することです。

- A. ネットワーク接続時に各デバイスにセキュリティ制御が適用されます
- B. ビジネスリーダーはセキュリティリスクを理解している
- C. ユーザーは利用規約を読み、署名済みです
- D. アプリケーションは実装前にテストされます

Answer: A ([メッセージを残す](#))

セクション : 情報システムの取得、開発、実装 説明/参照 :

最新問題: 667

The FIRST step in managing the risk of a cyber attack is to:

- A. assess the vulnerability impact.
- B. evaluate the likelihood of threats.
- C. identify critical information assets.
- D. estimate potential damage.

Answer: C ([メッセージを残す](#))

The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

最新問題: 668

監査の質を向上させるために、監査計画段階で上級監査責任者が関与する最良の方法は次のうちどれですか？

- A. 監査計画書を作成する。

- B. 提案された監査範囲を確認する。
- C. 被監査企業の経営陣と面談する。
- D. 計画立案の現場見学に参加する。

Answer: ([解答を表示する](#))

最新問題: 669

組織のセキュリティ意識向上プログラムの効果が向上したことを最もよく示しているのは、次のうちどれですか？

- A. 情報セキュリティ監査で指摘された事項の減少
- B. 意識向上研修を修了した職員数の増加
- C. 従業員から報告されたフィッシングメールの件数の増加
- D. マルウェアの発生件数の減少

Answer: ([解答を表示する](#))

組織のセキュリティ意識向上プログラムの効果は、ソーシャルエンジニアリング攻撃を認識して回避する能力など、脅威に対する人々の反応の変化に関するデータを収集することで測定できます¹。従業員から報告されるフィッシングメールの数の増加は、従業員がフィッシングの兆候とリスクをより認識し、そのような攻撃を防止または影響を軽減するために適切な行動をとる可能性が高いことを示しています²³。

参考文献

1: セキュリティ意識を測定することの重要性 2: セキュリティ意識向上プログラムの効果を測定する 3: セキュリティ意識向上トレーニングはどの程度効果的か？

組織のセキュリティ意識向上プログラムの効果は、ソーシャルエンジニアリング攻撃を認識して回避する能力など、脅威に対する人々の反応の変化に関するデータを収集することで測定できます¹。従業員から報告されるフィッシングメールの数の増加は、従業員がフィッシングの兆候とリスクをより認識し、そのような攻撃を防止または影響を軽減するために適切な行動をとる可能性が高いことを示しています²³。

参考文献

1: セキュリティ意識を測定することの重要性 2: セキュリティ意識向上プログラムの効果を測定する 3: セキュリティ意識向上トレーニングはどの程度効果的か？

最新問題: 670

次のうち、雷雨や騒音の大きい電気機器によって引き起こされる環境問題であり、コンピュータシステムのフリーズやクラッシュの原因にもなり得るものはどれですか？

- A. サグ
- B. ブラックアウト
- C. ブラウンアウト
- D. EMI

Answer: D ([メッセージを残す](#))

説明／参考資料：

雷雨やノイズの多い電気機器によって引き起こされる電磁干渉（EMI）。この干渉は、コンピュータシステムのフリーズやクラッシュ、さらには電圧降下、スパイク、サージによって引き起こされるものと同様の損傷を引き起こす可能性があります。

非シールドツイストペアケーブルは、シールドツイストペアケーブルのようなシールド構造を持たないため、外部の電氣的な干渉を受けやすく、信号の完全性が低下する可能性があります。

また、侵入者は送信データを傍受するために、ケーブルに盗聴器を取り付けたり、電線からの放射線を監視したりする可能性があります。そのため、UTPケーブルは、非常に機密性の高いデータを送信する場合や、電磁干渉 (EMI) や無線周波数干渉 (RFI) が多い環境に設置する場合には、適切な選択肢とは言えません。

欠点はあるものの、UTPケーブルは最も一般的なケーブルタイプです。UTPは安価で、設置時に簡単に曲げることができ、ほとんどの場合、上記の欠点によるリスクは、より高価なケーブルを使用する正当な理由にはなりません。

試験では、停電に関する以下の情報を知っておく必要があります。

完全停電 (ブラックアウト) - 電力供給が完全に途絶える状態。単一の建物から地域全体に至るまで発生する可能性があり、多くの場合、気象条件や電力会社がユーザーの需要を満たせないことが原因となる。

電圧の著しい低下 (ブラウンアウト) とは、電力会社が許容範囲内の電力を供給できなくなる状態を指します。このような障害は電子機器に負荷をかけ、機器の寿命を縮めたり、場合によっては永久的な損傷を引き起こしたりする可能性があります。

電圧低下、電圧急上昇、電圧サージ — 電圧レベルが一時的かつ急速に低下 (電圧低下または上昇 (電圧急上昇) および電圧サージ) する現象。これらの異常は、データの損失、データの破損、ネットワーク伝送エラー、またはハードウェア機器の物理的な損傷を引き起こす可能性があります。

電磁干渉 (EMI) - 雷雨やノイズの多い電気機器によって引き起こされる電磁干渉 (EMI)。この干渉により、コンピュータシステムがフリーズしたりクラッシュしたりするほか、電圧降下、スパイク、サージによって引き起こされるものと同様の損傷が発生する可能性があります。

以下の回答は誤りでした。

電圧低下 - 電圧が一時的に急激に低下すること。

完全停電 (ブラックアウト) - 電力供給が完全に途絶える状態。単一の建物から地域全体に至るまで発生する可能性があり、多くの場合、気象条件や電力会社がユーザーの需要を満たせないことが原因となる。

電圧の著しい低下 (ブラウンアウト) とは、電力会社が許容範囲内の電力を供給できなくなる状態を指します。このような障害は電子機器に負荷をかけ、機器の寿命を縮めたり、場合によっては永久的な損傷を引き起こしたりする可能性があります。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014 372ページ

そして

Hernandez CISSP、Steven (2012-12-21)。公式 (ISC)2 CISSP CBK ガイド、第 3 版 ((ISC)2 Press) (Kindle 位置 6507-6512)。Acerbic Publications。Kindle 版。

最新問題: 671

Which of the following should be the MOST important consideration in IT portfolio management?

- A. Aligning IT portfolio processes with corporate objectives
- B. Increasing the budget and resources allocated for IT investments
- C. Determining the opportunity cost of IT investment projects
- D. Selecting IT investment projects that align with corporate strategy

Answer: D ([メッセージを残す](#))

The most important consideration in IT portfolio management is ensuring that all IT investments directly support and align with the organization's corporate strategy. This alignment maximizes business value, ensures resource optimization, and helps prioritize projects that contribute to strategic objectives.

最新問題: 672

An organization is choosing key performance indicators (KPIs) for its information security management.

Which of the following KPIs would provide stakeholders with the MOST useful information about whether information security risk is being managed?

- A. Time from identifying a security threat to implementing a solution
- B. The number of security incidents during the past quarter
- C. The number of security controls implemented
- D. Time from initial reporting of an incident to appropriate escalation

Answer: A ([メッセージを残す](#))

最新問題: 673

Which of the following are BEST suited for continuous auditing?

- A. Manual transactions
- B. Irregular transactions
- C. Low-value transactions
- D. Real-time transactions

Answer: ([解答を表示する](#))

Section: The process of Auditing Information System

最新問題: 674

Which of the following is the MOST important audit activity following a database migration?

- A. Review backup processes and retention requirements for the original
- B. Perform an audit of the data migration scripts to ensure integrity of the database
- C. Analyze logs to identify potential migration errors that may have occurred
- D. Review decommissioning processes for the original source of data

Answer: C ([メッセージを残す](#))

最新問題: 675

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data.

A preliminary investigation revealed that the discrepancies were caused by problems with the organization ' s data quality

Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

- A. Data with customer personal information
- B. Data reported to the regulatory body
- C. Data supporting financial statements
- D. Data impacting business objectives

Answer: B ([メッセージを残す](#))

To ensure that management concerns are addressed, internal audit should recommend that the data quality team review the data reported to the regulatory body first. This is because this data set is the most relevant and critical to the issue that triggered the enhancement of the data quality program. The data reported to the regulatory body should be accurate, complete, consistent, and timely, as any discrepancies could result in fines, penalties, or reputational damage for the organization. Data with customer

personal information is important for data quality, but it is not directly related to the regulatory reporting issue. Data supporting financial statements is important for data quality, but it may not be the same as the data reported to the regulatory body. Data impacting business objectives is important for data quality, but it may not be as urgent or sensitive as the data reported to the regulatory body. References:

CISA Review Manual, 27th Edition, pages 404-4051

CISA Review Questions, Answers and Explanations Database, Question ID: 262

最新問題: 676

複数の拠点を持つ医療機関が、患者がどこで治療を受けても患者データにアクセスできるようにしたい場合、次のうちどれが最も効率的なソリューションでしょうか？

- A. 動的位置特定
- B. ネットワーク分割
- C. インフラストラクチャ・アズ・ア・サービス (IaaS) プロバイダー
- D. サービスとしてのソフトウェア (SaaS) プロバイダー

Answer: D ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 677

次のコンピュータネットワークのうち、都市内に限定されたWANはどれですか？

- A. LAN
- B. 男性
- C. SAN
- D. PAN

Answer: B ([メッセージを残す](#))

説明／参考資料：

MAN (メトロポリタンエリアネットワーク) とは、地理的に離れていても同一の都市圏内にあり、相互に接続されている2台以上のコンピュータ、通信機器、またはネットワークのことです。都市圏の範囲は地方自治体によって定められ、都市が大きいほどMANも大きくなり、都市が小さいほどMANも小さくなります。

試験に向けて、コンピュータネットワークに関する以下の情報を知っておく必要があります。

ローカルエリアネットワーク (LAN)

ローカルエリアネットワーク (LAN) とは、ネットワークメディアを使用して、家庭、学校、コンピュータラボ、オフィスビルなどの限られたエリア内のコンピュータを相互接続するコンピュータネットワークのことです。

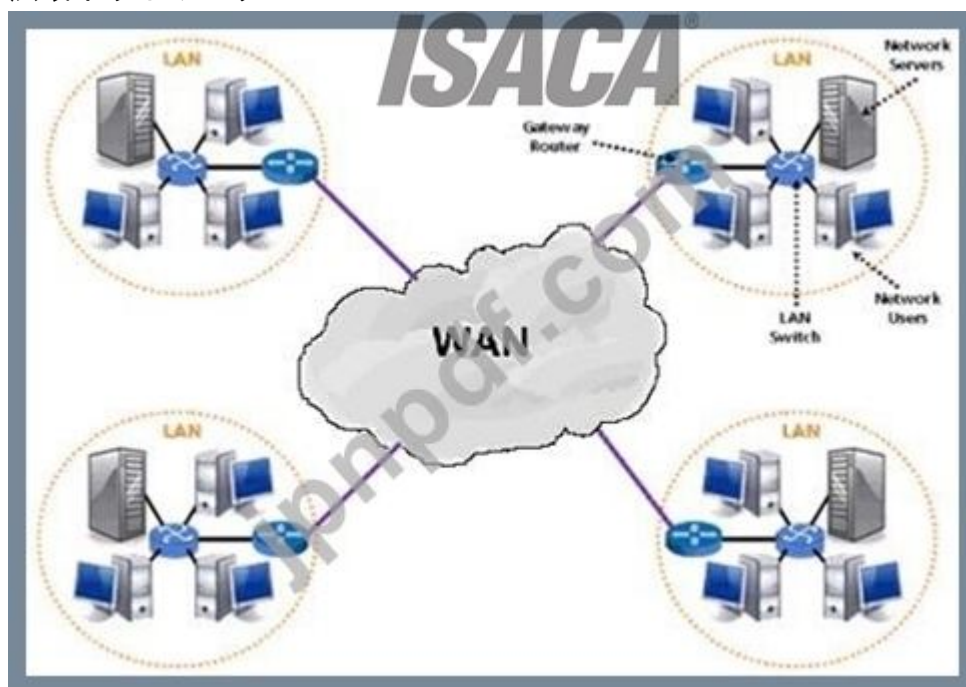
ローカルエリアネットワーク



広域ネットワーク

広域ネットワーク (WAN)とは、専用回線を使用して広範囲をカバーするネットワーク (つまり、都市圏、地域、国、または国際的な境界を越えて接続するあらゆる電気通信ネットワーク)のことです。

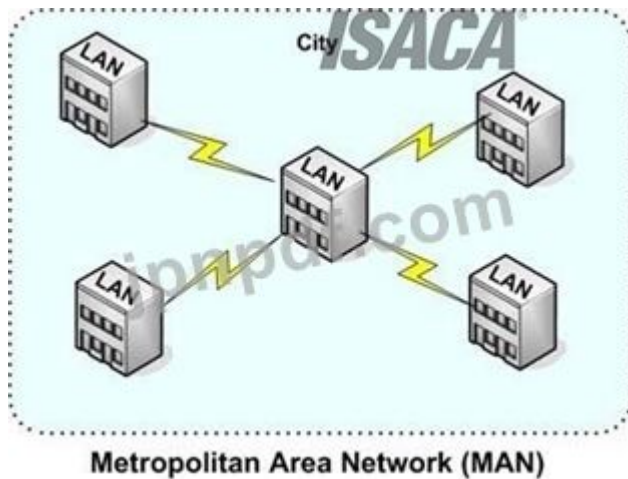
広域ネットワーク



画像出典 <http://www.netprivateer.com/images/lanwan.gif>

メトロポリタンエリアネットワーク

メトロポリタンエリアネットワーク (MAN)とは、地理的に離れていても同じ都市圏内にあり、相互に接続されている2台以上のコンピュータ、通信機器、またはネットワークのことです。都市圏の境界は地方自治体によって定められ、都市が大きいほどMANも大きくなり、都市が小さいほどMANも小さくなります。



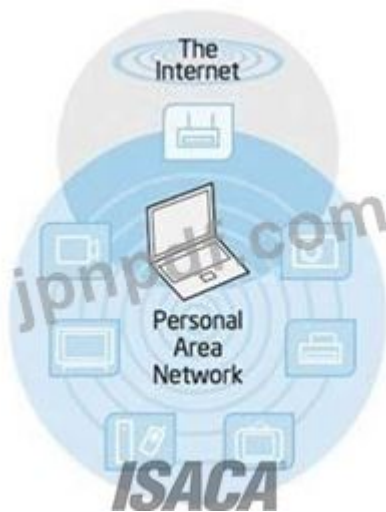
Metropolitan Area Network (MAN)

画像出典 <http://cis.msjc.edu/courses/images/MAN.jpg>

パーソナルエリアネットワーク

パーソナルエリアネットワーク (PAN)とは、コンピュータ、電話、携帯情報端末などのデバイス間でデータ伝送を行うためのコンピュータネットワークです。PANは、デバイス同士の通信 (デバイス内通信)や、上位ネットワークやインターネットへの接続 (アップリンク)に利用できます。

パーソナルエリアネットワーク

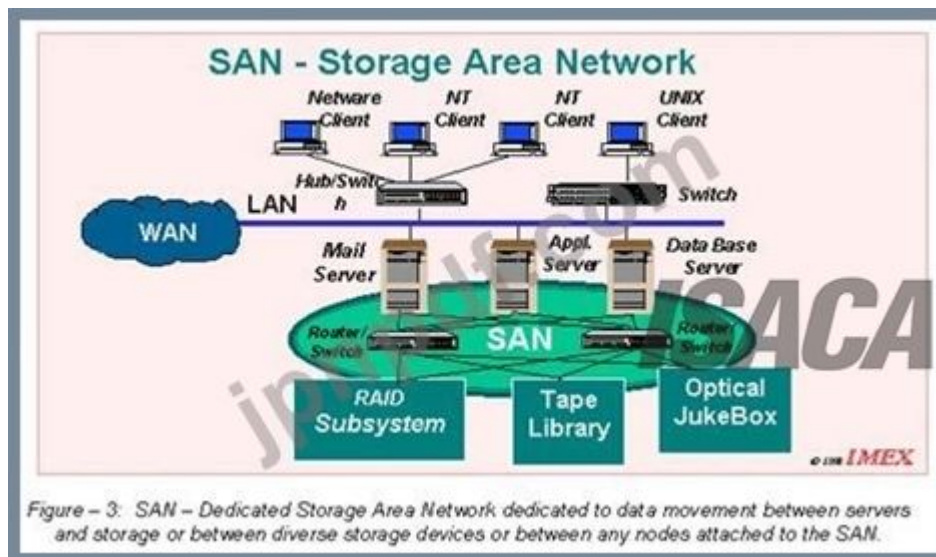


オリジナル画像はこちらをクリックしてください

ストレージエリアネットワーク

ストレージエリアネットワーク (SAN)は、統合されたブロックレベルのデータストレージへのアクセスを提供する専用ネットワークです。SANは主に、ディスクアレイ、テープライブラリ、光ディスクジュークボックスなどのストレージデバイスをサーバーからアクセス可能にし、オペレーティングシステムからローカル接続デバイスのように認識させるために使用されます。SANは通常、独自のストレージデバイスネットワークを持ち、他のデバイスからローカルエリアネットワーク (LAN) 経由でアクセスすることはできません。

ストレージエリアネットワーク



画像出典 <http://www.imexresearch.com/images/sasnassan-3.gif>

以下の回答は誤りでした。

PAN (パーソナルエリアネットワーク)とは、コンピュータ、電話、携帯情報端末などのデバイス間でデータ伝送を行うためのコンピュータネットワークです。PANは、デバイス同士の通信 (デバイス内通信)や、上位ネットワークやインターネットへの接続 (アップリンク)に利用できます。

LAN (ローカルエリアネットワーク)とは、ネットワークメディアを使用して、家庭、学校、コンピュータラボ、オフィスビルなどの限られたエリア内のコンピュータを相互接続するコンピュータネットワークのことです。

SAN (ストレージエリアネットワーク)とは、統合されたブロックレベルのデータストレージへのアクセスを提供する専用ネットワークです。SANは主に、ディスクアレイ、テープライブラリ、光ディスクジュークボックスなどのストレージデバイスをサーバーからアクセス可能にし、オペレーティングシステムからローカル接続デバイスのように認識させるために使用されます。SANは通常、独自のストレージデバイスネットワークを持ち、他のデバイスからはローカルエリアネットワーク (LAN) 経由でアクセスできません。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 258ページ

最新問題: 678

フィッシングシミュレーションテストを実施する究極の目的は次のうちどれですか？

- A. サイバーインシデントの発生確率を低減するため
- B. セキュリティ意識レベルの向上
- C. スпамフィルタリングをインストールする必要性をなくす
- D. サイバーイベントの発生を特定する

Answer: (解答を表示する)

最新問題: 679

An IS auditor is reviewing an organization's business intelligence infrastructure. The BEST recommendation to help the organization achieve a reasonable level of data quality would be to:

- A. review data against data classification standards.
- B. outsource data cleansing to skilled service providers.
- C. consolidate data stored across separate databases into a warehouse.

D. analyze the data against predefined specifications.

Answer: D ([メッセージを残す](#))

This is because analyzing the data against predefined specifications is a method of data quality assessment that can help the organization achieve a reasonable level of data quality. Data quality assessment is the process of measuring and evaluating the accuracy, completeness, consistency, timeliness, validity, and usability of the data. Predefined specifications are the criteria or standards that define the expected or desired quality of the data. By comparing the actual data with the predefined specifications, the organization can identify and quantify any gaps, errors, or deviations in the data quality, and take corrective actions accordingly¹².

Reviewing data against data classification standards (A) is not the best answer, because it is not a method of data quality assessment, but rather a method of data security management. Data classification standards are the rules or guidelines that define the level of sensitivity and confidentiality of the data, and determine the appropriate security and access controls for the data. For example, data can be classified into public, internal, confidential, or restricted categories. Reviewing data against data classification standards can help the organization protect the data from unauthorized or inappropriate use or disclosure, but it does not directly improve the data quality³.

Outsourcing data cleansing to skilled service providers (B) is not the best answer, because it is not a recommendation to help the organization achieve a reasonable level of data quality, but rather a decision to delegate or transfer the responsibility of data quality management to external parties. Data cleansing is the process of detecting and correcting any errors, inconsistencies, or anomalies in the data. Skilled service providers are third-party vendors or contractors that have the expertise and resources to perform data cleansing tasks. Outsourcing data cleansing to skilled service providers may have some benefits, such as cost savings, efficiency, or scalability, but it also has some risks, such as loss of control, dependency, or liability⁴.

Consolidating data stored across separate databases into a warehouse is not the best answer, because it is not a method of data quality assessment, but rather a method of data integration and storage. Data integration is the process of combining and transforming data from different sources and formats into a unified and consistent view. Data warehouse is a centralized repository that stores integrated and historical data for analytical purposes. Consolidating data stored across separate databases into a warehouse can help the organization improve the availability and accessibility of the data, but it does not necessarily improve the data quality.

最新問題: 680

IS監査担当者は、ネットワーク管理者による不正行為の可能性を特定しました。IS監査担当者は以下の対応を取るべきです。

- A. 迅速な解決を確実にするための報告書を発行する
- B. 他の議論を行う前に、監査委員会と監査結果について検討する。
- C. 監査結果を公表する前に、より詳細なテストを実施する
- D. 潜在的な監査結果をセキュリティ管理者と共有する

Answer: ([解答を表示する](#)**)**

セクション：情報システムの監査プロセス

最新問題: 681

以下のプライバシー原則のうち、データ管理者が個人データを意図しない方法で使用してデータ主体の保護を侵害しないことを保証するものはどれですか？

- A. データ保持

- B. 適切性
- C. 精度
- D. 目的制限

Answer: ([解答を表示する](#))

セクション：情報資産の保護

最新問題: 682

Which of the following ensures the availability of transactions in the event of a disaster?

- A. Send tapes hourly containing transactions offsite,
- B. Send tapes daily containing transactions offsite.
- C. Capture transactions to multiple storage devices.
- D. Transmit transactions offsite in real time.

Answer: D ([メッセージを残す](#))

The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

最新問題: 683

次の暗号化方式のうち、安全に配布された一対の鍵コードを使用し、単一のメッセージの暗号化と復号に一度だけ使用する方式はどれですか？

- A. フグ
- B. トリップワイヤー
- C. 証明書
- D. DES
- E. ワンタイムパッド
- F. 選択肢に該当しない。

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

暗号化技術を用いることで、送信中のメッセージを保護することが可能です。

暗号化方式の一つであるワンタイムパッドは、正しく使用すれば解読不可能であることが証明されている。

この方式では、安全に配布された一対の鍵コードを使用し、単一のメッセージのエンコードとデコードに一度だけ使用します。ただし、この方式は安全に利用するのが難しく、非常に不便です。

最新問題: 684

An organization using development operations (DevOps) processes has deployed tools to provide automated configuration management functionality. Which of the following is the BEST way to ensure changes to system configuration do not inadvertently introduce security vulnerabilities into production platforms?

- A. Implement logging of developer activity in the production environment.
- B. Implement mechanisms for measuring production application performance.

C. Implement tools to inventory newly introduced application components.

D. Implement automated scanning as part of the release process.

Answer: D ([メッセージを残す](#))

最新問題: 685

Which of the following control helps to identify an incident's activities and potentially an intruder?

A. Deterrent

B. Preventive

C. Detective

D. Compensating

Answer: ([解答を表示する](#))

Section: The process of Auditing Information System

Explanation:

Detective control helps identify an incident's activities and potentially an intruder

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers.

Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring

Compensating - Compensating Controls provide an alternative measure of control

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

最新問題: 686

Which of the following should be the IS auditor's PRIMARY focus when evaluating an organization's offsite storage facility?

- A. Retention policy and period
- B. Shared facilities
- C. Results of business continuity plan (BCP) tests
- D. Adequacy of physical and environmental controls

Answer: B ([メッセージを残す](#))

最新問題: 687

IPSECにおいて、暗号化アルゴリズム、鍵初期化ベクトル、鍵の有効期間など、通信当事者間で適用されるべきセキュリティパラメータを定義するのは次のうちどれですか？

- A. セキュリティパラメータインデックス (SPI)
- B. セキュリティ協会 (SA)
- C. カプセル化セキュリティペイロード (ESP)
- D. 認証ヘッダー (AH)

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

セキュリティアソシエーション (SA)は、暗号化アルゴリズム、鍵初期化ベクトル、鍵の有効期間など、通信当事者間で適用されるべきセキュリティパラメータを定義します。

試験では、IPSecプロトコルに関する以下の情報を知っておく必要があります。

IPネットワーク層パケットセキュリティプロトコルは、トランスポートモードおよびトンネルモードの暗号化方式を用いてVPNを確立する。

転送方式では、各パケットのデータ部分が暗号化されます。IPsecにおける暗号化はカプセル化セキュリティペイロード (ESP)と呼ばれ、ESPがプロセス全体の機密性を提供します。

トンネルモードでは、ESPペイロードとそのヘッダーは暗号化されます。否認防止を実現するため、追加の認証ヘッダー (AH)が適用されます。

IPSecセッションをどちらのモードで確立する場合でも、セキュリティアソシエーション (SA)が確立されます。SAは、暗号化アルゴリズム、キー初期化ベクトル、キーの有効期間など、通信当事者間で適用すべきセキュリティパラメータを定義します。これは、それぞれESPヘッダーまたはAHヘッダー内に定義されます。SAは、送信ホスト内で32ビットのセキュリティパラメータインデックス (SPI)フィールドが定義されたときに確立されます。SPIは一意の識別子であり、送信ホストが指定されたセキュリティパラメータを参照し、受信ホストに適用できるようにします。

IPSecは、インターネットセキュリティアソシエーションおよび鍵管理プロトコル/オークリー (ISAKMP/Oakley)を用いた非対称暗号化によって、より安全になります。ISAKMP/Oakleyは、鍵の自動管理、公開鍵の使用、SAおよび属性の交渉、確立、変更、削除を可能にします。認証には、送信側はデジタル証明書を使用します。SAおよび暗号鍵の生成、認証、配布をサポートすることで、接続の安全性が確保されます。

以下の回答は誤りでした。

セキュリティパラメータインデックス (SPI) - セキュリティパラメータインデックス (SPI)は、送信ホストが適用するセキュリティパラメータを参照できるようにする一意の識別子です。

カプセル化セキュリティペイロード (ESP) - カプセル化セキュリティペイロード (ESP)は、送信者の認証とデータの暗号化をサポートするために使用されます。

認証ヘッダー (AH) - 認証ヘッダーは、データの送信者の認証を可能にします。

参照：

CISAレビューマニュアル2014年版 353ページ

最新問題: 688

What is the PRIMARY purpose of performing a parallel run of a new system?

- A. To validate the operation of the new system against its predecessor.
- B. To verify the new system provides required business functionality
- C. To verify the new system can process the production load
- D. To provide a failover plan in case of system issues.

Answer: ([解答を表示する](#))

最新問題: 689

During an IT governance audit, an IS auditor notes that IT policies and procedures are not regularly reviewed and updated. The GREATEST concern to the IS auditor is that policies and procedures might not:

- A. reflect current practices.
- B. be subject to adequate quality assurance (QA).

C. include new systems and corresponding process changes.

D. incorporate changes to relevant laws.

Answer: D ([メッセージを残す](#))

Regulations and laws are important external issues that cannot be ignored or avoided.

最新問題: 690

次のファイアウォールのうち、各ネットワークフレームまたはパケットを個別に処理するのはどれですか？

A. ステートフルファイアウォール

B. ハードウェアファイアウォール

C. 複合ファイアウォール

D. パケットフィルタリングファイアウォール

E. ステートレスファイアウォール

F. 選択肢に該当しない。

Answer: E ([メッセージを残す](#))

ステートレスファイアウォールは、各ネットワークフレームまたはパケットを個別に処理します。

このようなファイアウォールは、特定のパケットが既存の接続の一部であるかどうかを知る方法がありません。

新しい接続を確立しようとしているのか、それとも単なる不正なパケットなのか。

最新問題: 691

Which of the following measures can effectively minimize the possibility of buffer overflows?

A. Sufficient bounds checking

B. Sufficient memory

C. Sufficient processing capability

D. Sufficient code injection

E. None of the choices

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

バッファオーバーフローは、プロセスのクラッシュや誤った結果の発生を引き起こす可能性があります。これは、悪意のあるコードを実行したり、プログラムを意図しない動作をさせたりするように特別に設計された入力によって引き起こされることがあります。そのため、バッファオーバーフローは多くのソフトウェアの脆弱性の原因となり、多くのエクスプロイトの基盤となっています。

プログラマまたはコンパイラによる適切な境界チェックを行うことで、バッファオーバーフローを防ぐことができます。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 692

物理的なアクセス制御は、通常、以下のどの方法に基づいて実装されますか 2つ選択してください。

- A. 機械式錠
- B. 警備員
- C. オペレーティングシステム
- D. トランザクションアプリケーション
- E. 選択肢のどれもでない。

Answer: A,B ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

物理セキュリティにおいて、アクセス制御とは、許可された人物以外の立ち入りを制限する措置を指す。人的手段による執行には、警備員、用心棒、受付係などが含まれる。機械的手段には、錠前と鍵。

最新問題: 693

IS監査人が監査対象領域における統制の有効性を判断する上で、最も有効な手段は次のうちどれですか？

- A. SWOT分析
- B. 制御実装方法
- C. 過去の監査結果
- D. 自己評価 (CSA)

Answer: D ([メッセージを残す](#))

最新問題: 694

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

- A. Parallel
- B. Preparedness
- C. Walk-thorough
- D. Paper

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

最新問題: 695

Several unattended laptops containing sensitive customer data were stolen from personnel offices Which of the following would be an IS auditor's BEST recommendation to protect data in case of recurrence?

- A. Encrypt the disk drive.

- B. Require two-factor authentication
- C. Enhance physical security
- D. Require the use of cable locks

Answer: A ([メッセージを残す](#))

According to the CISA - Certified Information Systems Auditor Study Guide¹, the correct answer to your question is A. Encrypt the disk drive. This is because encryption is a logical security measure that can protect data even if the physical device is stolen or lost. Encryption makes the data unreadable and inaccessible without the proper key or password. The other options are not as effective as encryption in this scenario. Two- factor authentication is a user authentication method that requires two pieces of evidence to verify the user's identity, such as a password and a code sent to a phone. However, this does not prevent unauthorized access to the data if the laptop is already logged in or if the attacker can bypass the authentication. Enhancing physical security is a preventive measure that can reduce the risk of theft, but it does not guarantee that theft will not occur or that the data will be safe if it does. Requiring the use of cable locks is another preventive measure that can deter thieves, but it can also be easily cut or removed by a determined attacker.

最新問題: 696

特定された事業リスクの管理において、内部監査機能の主要な役割として、次のうちどれが適切でしょうか？

- A. リスク許容度を確立する
- B. 企業リスクマネジメント (ERM) の検証
- C. リスク管理フレームワークの構築
- D. リスク管理フレームワークの運用

Answer: B ([メッセージを残す](#))

最新問題: 697

Which of the following is the BEST review for an IS auditor to conduct when a vulnerability has been exploited by an employee?

- A. Compliance audit
- B. Application security testing
- C. Forensic audit
- D. Penetration testing

Answer: C ([メッセージを残す](#))

Comprehensive and Detailed Step-by-Step Explanation:

When an employee exploits a vulnerability, the most appropriate audit is a forensic audit, as it focuses on investigating and documenting security incidents for legal or disciplinary action.

- * Option A (Incorrect): A compliance audit ensures adherence to policies but does not investigate incidents in detail.
- * Option B (Incorrect): Application security testing helps identify vulnerabilities but does not address employee misuse.
- * Option C (Correct): A forensic audit gathers digital evidence, determines how the exploit occurred, and ensures legal compliance in the investigation.
- * Option D (Incorrect): Penetration testing identifies weaknesses but does not analyze past incidents.

Reference: ISACA CISA Review Manual -Domain 5: Protection of Information Assets- Covers forensic investigations, digital evidence collection, and security incident response.

最新問題: 698

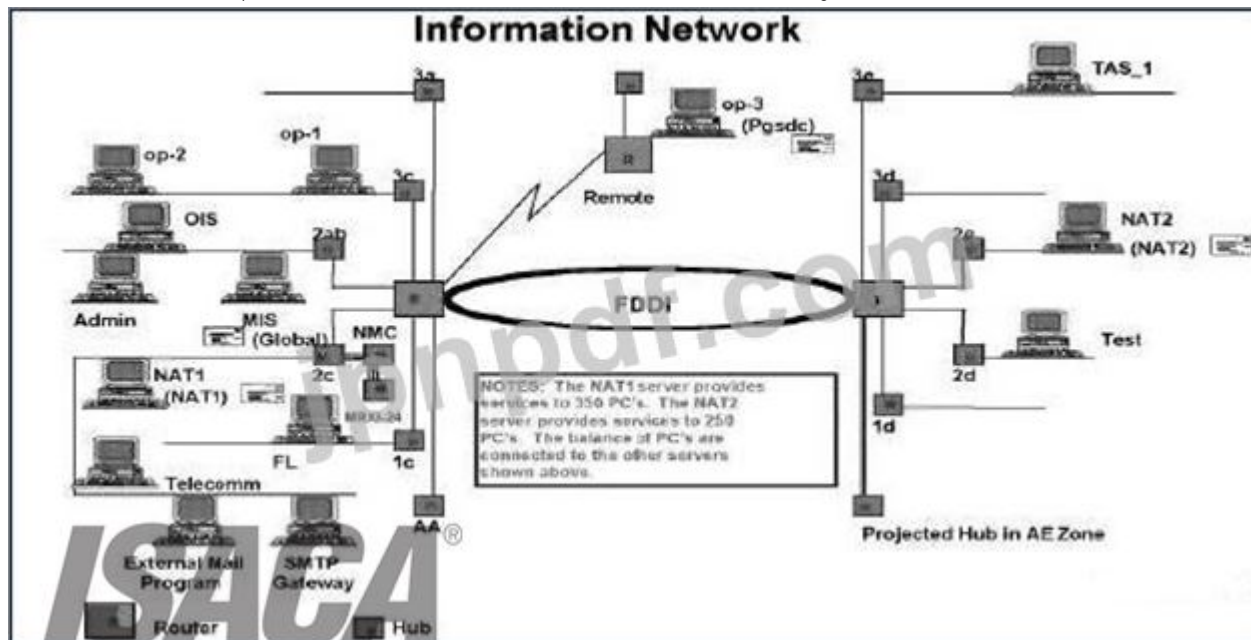
To BEST determine if a project is successfully addressing business requirements while managing the associated risk, which of the following should an IS auditor expect to find at each significant milestone?

- A. A revised business impact and risk analysis
- B. Formal acceptance by appropriate stakeholders
- C. Post-implementation review with affected parties
- D. Comprehensive end user acceptance testing

Answer: B ([メッセージを残す](#))

最新問題: 699

図の2c領域には、互いに接続された3つのハブがあります。これはどのような潜在的なリスクを示している可能性がありますか？



- A. ウイルス攻撃
- B. 性能低下
- C. 管理統制の不備
- D. 外部ハッカーに対する脆弱性

Answer: B ([メッセージを残す](#))

ハブは通常、外部と直接接続できない内部デバイスであるため、ハッカーの攻撃を受けにくい。ハブ攻撃に特化した既知のウイルスは存在しない。このような状況は管理体制の不備を示す可能性もあるが、ハブを複数台接続して端末接続を増やすような運用が行われている場合は、選択肢Bの方が可能性が高い。

最新問題: 700

次の監査手順のうち、電子商取引アプリケーションシステムの編集ルーチンの有効性を評価する上で最も決定的なのはどれですか？

- A. ソースコードのレビュー
- B. 知識豊富なユーザーへのインタビュー
- C. プログラムドキュメントのレビュー
- D. テストランザクションの使用

Answer: A ([メッセージを残す](#))

最新問題: 701

IS監査担当者にとって、ソフトウェアリリース管理プロセスを理解することは非常に重要です。次のうち、通常、重要な変更や新機能の追加が含まれるソフトウェアリリースはどれですか？

- A. メジャーソフトウェアリリース
- B. マイナーソフトウェアリリース
- C. 緊急ソフトウェアリリース
- D. 一般ソフトウェアリリース

Answer: ([解答を表示する](#))

説明／参考資料：

メジャーリリースでは通常、新しい機能や機能が追加されます。メジャーリリースには、以前のマイナーリリースで行われたすべての変更が集約される場合があります。メジャーリリースでは、バージョン番号が1つ上がります。例えば、バージョン5.70からバージョン6に上がります。

CISA試験では、ソフトウェアリリース管理に関して以下の情報を知っておく必要があります。

ソフトウェアリリース管理とは、リリースが確実に計画、スケジュールされ、テスト環境および本番環境へ正常に移行（展開されることを保証するプロセスです。ソフトウェアリリース管理は、単に「本番環境への移行プロセスを自動化する」ことだけではありません。もちろんそれも重要な要素ですが）。リリースをコンテナとして活用し、アプリケーションの変更を包括的に捉え、変更が再現可能かつ管理された方法でパッケージ化、リリース、テストされることを保証することも重要です。

リリース管理は、オーケストラの指揮者に例えられることが多く、個々の変更はオーケストラ内の様々な楽器に相当します。ソフトウェアリリース管理は、より広く理解され、普及しているソフトウェア変更管理や構成管理といった分野と密接に関連しています。

ソフトウェアリリース管理とは、ソフトウェアをユーザーに提供するプロセスです。構成アイテムの各更新またはアップグレードは、リリースと呼ばれます。

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release - Not a valid type of software release.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 244

最新問題: 702

An IS auditor is concerned that unauthorized access to a highly sensitive data center might be gained by piggybacking or tailgating. Which of the following is the BEST recommendation? (Choose Correct answer and give explanation from CISA Certification - Information Systems Auditor official book)

- A. Biometrics
- B. Procedures for escorting visitors
- C. エアロック入口
- D. 侵入警報器

Answer: [\(解答を表示する\)](#)

ピギーバックとテールゲーティングは、不正アクセスによく用いられる2つの手法で、いずれも正規のユーザーに続いてセキュリティチェックを受けずに安全なエリアに侵入するものです。これを防ぐため、組織はデータセンターへの訪問者を案内し、滞在中の行動を監視する手順を整備する必要があります。これにより、不正ユーザーが機密性の高いデータセンターにアクセスすることを確実に防ぐことができます。

最新問題: 703

Which of the following BEST demonstrates to an IS auditor that an organization has implemented effective risk management processes?

- A. Critical business assets have additional controls.
- B. The risk register is reviewed periodically.
- C. A business impact analysis (BIA) has been completed.
- D. The inventory of IT assets includes asset classification.

Answer: B [\(メッセージを残す\)](#)

Section: The process of Auditing Information System

最新問題: 704

便乗リスクに対処するための最も効果的な対策は次のとおりです。

- A. 受付係がいる単一の入り口。
- B. スマートカードの使用。
- C. 生体認証ドアロック。
- D. デッドマンドア。

Answer: D [\(メッセージを残す\)](#)

デッドマンドアとは、2枚のドアを使用するシステムです。2枚目のドアが作動するには、1枚目のドアが閉まり、施錠され、待機エリアAには1人しか立ち入ることができない状態になっている必要があります。これにより、許可された人物に続いて許可されていない人物がセキュリティエリアに侵入する（ピギーバック）リスクが軽減されます。その他の選択肢はすべてセキュリティエリアへの入退室を物理的に制御するものですが、ピギーバックのリスクには特に対処していません。

最新問題: 705

パスワードを変更するのに適した時期は次のうちどれですか？

- A. 180～365日ごと
- B. 30～45日ごと
- C. 10～20日ごと
- D. 90～120日ごと
- E. 選択肢のどれでもない。

Answer: D ([メッセージを残す](#))

パスワードは、データと情報を保護するための最初の防衛線です。ユーザーには、パスワードがどのような機能を提供し、パスワードを使って何ができるのかを理解してもらう必要があります。また、良いパスワードと悪いパスワードの違いについても理解してもらう必要があります。良いパスワードは、大文字と小文字の英字、数字、記号を組み合わせたものです。パスワードは8文字以上を使用してください。定期的にパスワードクラッカープログラムを実行し、簡単に解読できるパスワードはすぐに変更するようユーザーに求めることをお勧めします。いずれにしても、90日から120日ごとにパスワードを変更するように促してください。

最新問題: 706

被験者の身元を確認するためにどのようなプロセスが使用されますか？

- A. 識別
- B. 否認禁止
- C. 認証
- D. 認証

Answer: ([解答を表示する](#)**)**

認証は、対象者の身元を確認するために使用される。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfumps**)

最新問題: 707

ある組織は基幹アプリケーションの開発を外部委託しました。しかし、その組織はアプリケーションのサポートと将来の保守を社内に戻す予定です。IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？

- A. アウトソーシングのコストは、社内開発よりも低い。
- B. ベンダーの開発チームは海外に拠点を置いています。
- C. ビジネスユーザー向けの研修計画は策定されていません。
- D. データモデルが明確に文書化されていません。

Answer: D ([メッセージを残す](#))

IS監査担当者が最も懸念すべき点は、データモデルが明確に文書化されていないことである。

データモデルとは、アプリケーションで使用されるデータの構造、関係性、および制約を表現したものです。データの正確性、一貫性、および品質を確保する上で重要な役割を果たすため、ソフトウェア開発プロセスにおいて不可欠な要素です。データモデルの明確かつ包括的なドキュメントは、データの理解、変更、およびアプリケーションロジックのトラブルシューティングを容易にするため、アプリケーションの保守とサポートに不可欠です。

組織がアプリケーションのサポートと将来のメンテナンスを社内で行うことを計画している場合、ベンダーからデータモデルのドキュメントを入手する必要があります。それがなければ、組織はベンダーから社内チームへの知識とスキルの移転、および変化するビジネスニーズと要件に合わせてアプリケーションを適応および強化することに困難に直面する可能性があります³。データモデルのドキュメントがないと、データとアプリケーションのパフォーマンスにおけるエラー、不整合、非効率のリスクも高まる可能性があります²。

その他の調査結果は、データモデルのドキュメント不足ほど懸念すべきものではありません。なぜなら、それらはアプリケーションの品質と保守性に直接影響しないからです。アウトソーシングのコストが社内開発よりも低いことは、組織にとってリスクではなくメリットです。これは、アウトソーシングによって組織の時間とコストが節約されたことを意味するからです⁴。ベンダーの開発チームが海外に所在することは、アウトソーシングでは一般的な慣行であり、必ずしもアプリケーションの品質低下やリスク増加を意味するものではありません。ただし、コミュニケーション、調整、文化の違いに関して課題が生じる可能性があり、明確な期待、役割、責任を確立し、効果的なコミュニケーションおよびコラボレーションツールと方法を使用することで対処できます⁵。ビジネスユーザー向けのトレーニングプランが作成されていないことは、アプリケーションを展開する前に組織が対処すべきギャップです。これは、アプリケーションのユーザー受容と満足度に影響を与える可能性があるためです。ただし、アプリケーション自体の品質や保守性に直接影響するものではありません。参考文献:

データモデリングとは？定義と種類 | Informatica¹

データモデリングのベストプラクティス :ドキュメント作成 | erwin²

データモデルのドキュメント - 概要 | ScienceDirect Topics³

アプリ開発のアウトソーシングのメリットとデメリット - Droids On Roids⁴

ソフトウェア開発アウトソーシングの8つのリスクとその対策 - Acropolisium⁵ ソフトウェアトレーニングプラン：自社向けプランの作成方法 - Elinext

最新問題: 708

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- A. Personal firewall
- B. Antivirus programs
- C. Intrusion detection system (IDS)
- D. Virtual local area network (VLAN) configuration

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

An intrusion detection system (IDS) would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator. Antivirus programs, personal firewalls and VIAN configurations would be later in the line of defense.

最新問題: 709

Which of the following would be the GREATEST concern to an IS auditor when reviewing the outsourcing contract for an organization's cloud service provider?

- A. There is no change management process defined in the contract.
- B. There are no procedures for incident escalation.
- C. There is no dispute resolution process defined in the contract.
- D. There is no right-to-audit clause defined in the contract.

Answer: D ([メッセージを残す](#))

The absence of a right-to-audit clause in the outsourcing contract for a cloud service provider would be of greatest concern to an IS auditor¹. This clause gives the client the right to audit the service provider's activities that are relevant to the services being provided¹. It is crucial for ensuring that the service provider is complying with the terms of the contract and meeting the client's standards for performance, security, and other aspects¹. Without this clause, the client may not be able to effectively monitor and manage risks associated with the outsourcing arrangement¹.

References:

Audit rights in outsourcing: certifications and third party reports

最新問題: 710

以下のどの手法が、IS監査担当者がアプリケーション内のセキュリティ脆弱性を検出するのに最も効果的ですか？

- A. 脅威モデリング
- B. コンセプトマッピング
- C. プロトタイピング
- D. 脅威インテリジェンス

Answer: ([解答を表示する](#)**)**

脅威モデリングとは、情報システム監査担当者が、脅威、攻撃、脆弱性、および対策を理解することで、アプリケーション内の潜在的なセキュリティ脆弱性を特定、分析、軽減できるようにする手法です。この予防的な手法は、安全なアプリケーションの設計に役立ちます。

参考文献

* ISACA CISAレビューマニュアル第27版、276～277ページ（脅威モデリング）

最新問題: 711

ハッシュ化と暗号化の最も重要な違いは、ハッシュ化では次の点です。

- A. 不可逆です。
- B. 出力は元のメッセージと同じ長さです。
- C. 完全性とセキュリティに関心があります。
- D. 送信側と受信側で同じです。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

ハッシュ化は一方方向的に機能します。メッセージにハッシュアルゴリズムを適用することで、メッセージのハッシュ値（ダイジェスト）が生成されます。

同じハッシュアルゴリズムをメッセージダイジェストに適用しても、元のメッセージは得られません。そのため、ハッシュ化は不可逆ですが、暗号化は可逆です。これがハッシュ化と暗号化の基本的な違いです。ハッシュ化は元のメッセージよりも小さい出力を生成しますが、暗号化は元のメッセージと同じ長さの出力を生成します。ハッシュ化はメッセージの完全性を検証するために使用され、セキュリティには対応していません。メッセージのハッシュ/ダイジェストを生成および検証するために、送信側と受信側で同じハッシュアルゴリズムが使用されます。暗号化では、暗号化と復号化に必ずしも送信側と受信側で同じアルゴリズムが使用されるとは限りません。

最新問題: 712

アプリケーション開発の初期段階で、最も難しい部分は何でしょうか？

- A. ソフトウェアの設定
- B. セキュリティ計画
- C. 時間とリソースの要件を決定する
- D. ハードウェアの設定

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

アプリケーション開発プロジェクトに必要な時間とリソースを決定することは、アプリケーション開発の初期段階において最も難しい部分であることが多い。

最新問題: 713

IS監査担当者は、アプリケーションサーバーのセキュリティ設定に一貫性がなく、潜在的な問題につながる可能性があることを発見した。

脆弱性。IS監査担当者による最適な推奨事項は次のうちどれですか？

- A. 変更管理プロセスを改善する
- B. 構成レビューを実施する
- C. セキュリティ指標を確立する
- D. 侵入テストを実施する

Answer: ([解答を表示する](#))

セクション：情報システムの監査プロセス

最新問題: 714

Which of the following is MOST important to determine when conducting an audit Of an organization's data privacy practices?

- A. Whether a disciplinary process is established for data privacy violations
- B. Whether strong encryption algorithms are deployed for personal data protection
- C. Whether privacy technologies are implemented for personal data protection
- D. Whether the systems inventory containing personal data is maintained

Answer: D ([メッセージを残す](#))

Explanation

The answer D is correct because the most important thing to determine when conducting an audit of an organization's data privacy practices is whether the systems inventory containing personal data is maintained.

A systems inventory is a list of all the systems, applications, databases, and devices that store, process, or transmit personal data within the organization. Maintaining a systems inventory is essential for data privacy because it helps the organization to identify, classify, and protect the personal data it holds, as well as to comply with the relevant privacy laws and regulations. A systems inventory also enables the organization to perform data protection impact assessments (DPIAs), data breach notifications, data subject access requests, and data retention and disposal policies.

他の選択肢は、選択肢 D ほど重要ではありません。データプライバシー違反に対する懲戒手続きが確立されているかどうか (選択肢 A) は、データプライバシー規則に違反した従業員を抑止または制裁する可能性のあるポリシー上の問題ですが、組織のデータプライバシー慣行に直接影響を与えるものではありません。個人データ保護のために強力な暗号化アルゴリズムが導入されているかどうか (選択肢 B) は、個人データのセキュリティと機密性を高める可能性のある技術的な問題ですが、正確性、同意、目的制限などのデータプライバシーの他の側面には対応していません。個人データ保護のためにプライバシー技術が導入されているかどうか (選択肢 C) も、組織のデータプライバシー慣行をサポートする可能性のある技術的な問題ですが、組織がベストプラクティスに従っていることや、適用される法律や規制を遵守していることを保証するものではありません。

参考文献：

IS監査の基礎 :データプライバシーの監査

プライバシー監査のベストプラクティス

ISACAがデータプライバシーとモバイルコンピューティングに関する新たな監査 保証プログラムを発表

最新問題: 715

Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

- A. protect the organization from viruses and nonbusiness materials.
- B. maximize employee performance.
- C. safeguard the organization's image.
- D. assist the organization in preventing legal issues

Answer: A ([メッセージを残す](#))

The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A.

Choices C and D are secondary or indirect benefits.

最新問題: 716

What must an IS auditor understand before performing an application audit?

- A. The potential business impact of application risks.
- B. Application risks must first be identified.
- C. Relative business processes.
- D. Relevant application risks.

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

An IS auditor must first understand relative business processes before performing an application audit.

最新問題: 717

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- A. Replay
- B. Brute force
- C. Cryptographic
- D. Mimic

Answer: [\(解答を表示する\)](#)

Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access. A brute force attack involves feeding the biometric capture device numerous different biometric samples. A cryptographic attack targets the algorithm or the encrypted data, in a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user, such as forging a signature or imitating a voice.

最新問題: 718

セキュリティ監査において、データの機密性が適切に管理されていることを確認するために、以下のうちどれをレビューすることが最も重要ですか？

- A. アクセス制御
- B. データフロー
- C. アクセスログの監視
- D. ネットワーク構成

Answer: A [\(メッセージを残す\)](#)

最新問題: 719

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

- A. Piggybacking
- B. Shoulder surfing
- C. Dumpster diving
- D. Impersonation

Answer: A [\(メッセージを残す\)](#)

Explanation/Reference:

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have their badge read at every controlled door no unauthorized person could enter the sensitive area. A. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

最新問題: 720

Which of the following should be of GREATEST concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system?

- A. Data conversion was performed using manual processes
- B. Backups of the old system and data are not available online
- C. The change management process was not formally documented
- D. Unauthorized data modifications occurred during conversion,

Answer: D ([メッセージを残す](#))

最新問題: 721

An IS auditor should recommend the use of library control software to provide reasonable assurance that:

- A. program changes have been authorized.
- B. only thoroughly tested programs are released.
- C. modified programs are automatically moved to production.
- D. source and executable code integrity is maintained.

Answer: ([解答を表示する](#)**)**

Explanation/Reference:

Explanation:

Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 722

Which of the following is the BEST reason for delaying the application of a critical security patch?

- A. Lack of vulnerability management
- B. Conflicts with software development life cycle
- C. Technology interdependencies
- D. Resource limitations

Answer: ([解答を表示する](#)**)**

Section: Information System Operations, Maintenance and Support

Explanation/Reference:

最新問題: 723

監査中に、情報システム監査担当者は、中規模組織のIT部門に独立したリスク管理機能がなく、組織の運用リスクに関する文書には、大まかに記述されたITリスクがいくつか含まれていないことに気づきました。このような状況で最も適切な推奨事項は何でしょうか？

- A. 外部のリスク管理専門家の協力を得て、ITリスク管理部門を設立し、ITリスクフレームワークを構築する。
- B. 業界標準の一般的な補助ツールを使用して、既存のリスク文書を扱いやすい複数の個別のリスクに分割します。
- C. 現在のやり方は中規模組織に適しているため、特に推奨事項はありません。
- D. 定期的なITリスク管理会議を開催し、リスクを特定・評価し、組織のリスク管理へのインプットとして軽減計画を作成する。

Answer: D ([メッセージを残す](#))

定期的な会議を設定することは、中規模組織におけるリスクを特定および評価し、それぞれの経営陣に責任を負わせ、リスクリストと軽減計画を最新の状態に保つための最良の方法です。中規模組織には通常、独立したITリスク管理部門はありません。さらに、リスクは通常、外部の支援を必要としないほど十分に管理可能です。一般的なリスクは一般的な業界標準でカバーされているかもしれませんが、組織の特定の状況には対応できません。組織内部からの詳細な評価なしには、個々のリスクは発見されません。1つのリスクポジションを複数に分割するだけでは不十分です。

最新問題: 724

Why is one-time pad not always preferable for encryption (choose all that apply):

- A. it is difficult to use securely.
- B. it is highly inconvenient to use.
- C. it requires licensing fee.
- D. it requires internet connectivity.
- E. it is Microsoft only.
- F. None of the choices.

Answer: ([解答を表示する](#)**)**

It's possible to protect messages in transit by means of cryptography. One method of encryption --the one-time pad --has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

最新問題: 725

以下のうち、意図せず機密情報が漏洩する可能性のあるものはどれですか？最も適切な回答を選択してください。

- A. 従業員が企業の情報セキュリティポリシーを認識していない
- B. 企業の情報セキュリティポリシーを遵守しなかった場合
- C. 一瞬の理性の喪失
- D. セキュリティポリシーの実施手順の欠如

Answer: A ([メッセージを残す](#))

説明／参考資料：

従業員が企業の情報セキュリティポリシーを認識していないと、意図せず機密情報が漏洩する可能性がある。

最新問題: 726

組織内のセキュリティ意識を高め、全従業員に適切なセキュリティ知識を提供することで、以下の攻撃のうちどれを回避できるでしょうか？

- A. サーフアタック
- B. 交通分析
- C. フィッシング
- D. 割り込み攻撃

Answer: C (メッセージを残す)

説明／参考資料：

フィッシングの手法には、ソーシャルエンジニアリング、リンク操作、スパイフィッシング、ホエーリング、ディッシング、ウェブサイト偽造などの手法が含まれる。

試験を受けるにあたっては、以下の情報を知っておく必要があります。

フィッシングとは、電子通信において信頼できる組織になりすまし、ユーザー名、パスワード、クレジットカード情報（場合によっては間接的に金銭）などの機密情報を入手しようとする行為です。人気のあるソーシャルウェブサイト、オークションサイト、銀行、オンライン決済処理業者、IT管理者などを装った通信が、疑いを持たない一般ユーザーを誘い込むためによく利用されます。フィッシングメールには、マルウェアに感染したウェブサイトへのリンクが含まれている場合があります。フィッシングは通常、メールのなりすましやインスタントメッセージングによって行われ、多くの場合、ユーザーを偽のウェブサイトに誘導します。偽のウェブサイトは、見た目や操作感が正規のウェブサイトとほぼ同じです。フィッシングは、ユーザーを欺くために使用されるソーシャルエンジニアリング手法の一例であり、現在のウェブセキュリティ技術の使い勝手の悪さを悪用しています。報告されるフィッシング事件の増加に対処するための取り組みには、法整備、ユーザー教育、啓発活動、技術的なセキュリティ対策などがあります。

スパイフィッシング

特定の個人や企業を標的としたフィッシング攻撃は、スパイフィッシングと呼ばれている。

攻撃者は、成功確率を高めるために、標的に関する個人情報収集する可能性がある。

リンク操作

フィッシングのほとんどの手法は、電子メール内のリンク（およびリンク先の偽のウェブサイト）が偽装された組織のものであるように見せかけるための何らかの技術的な欺瞞を利用しています。スペルミスのあるURLやサブドメインの使用は、フィッシングでよく使われる手口です。次の例のURL、<http://www.yourbank.example.com/> では、このURLが銀行のウェブサイトのサンプルセクションに誘導するように見えますが、実際にはこのURLはサンプルウェブサイトの「your bank」（つまりフィッシング）セクションを指しています。もう1つのよくある手口は、リンクの表示テキスト（タグ間のテキスト）が信頼できる宛先を示唆するように見せかけ、実際にはフィッシングサイトに誘導することです。次の例のリンク、[//en.wikipedia.org/wiki/Genuine](http://en.wikipedia.org/wiki/Genuine) は、「Genuine」というタイトルの記事にユーザーを誘導するように見えますが、クリックすると実際には「Deception」というタイトルの記事に移動します。ほとんどのブラウザの左下隅で、ユーザーはリンクがどこに誘導されるかをプレビューして確認できます。リンクの上にカーソルを数秒間重ねると似たような動作をすることがありますが、これはHTMLのツールチップタグを通してフィッシングサイト側で設定されている可能性があります。

ウェブサイトの偽造

被害者がフィッシングサイトにアクセスしたからといって、詐欺が終わるわけではありません。フィッシング詐欺の中には、JavaScriptコマンドを使ってアドレスバーを変更するものがあります。これは、正規のURLの画像をアドレスバーの上に重ねたり、元のアドレスバーを閉じて正規のURLが表示された新しいアドレスバーを開いたりすることで行われます。攻撃者は、信頼できるウェブサイトのスクリプトの脆弱性を悪用して、被害者を攻撃することさえ可能です。こうした攻撃（クロスサイトスクリプティングと呼ばれる）は、ユーザーを銀行やサービスのウェブページに誘導し、ウェブアドレスからセキュリティ証明書まで全てが正しく見えるように仕向けるため、特に厄介です。実際には、ウェブサイトへのリンクは攻撃を実行するために細工されており、専門知識がなければ見抜くのは非常に困難です。

以下の回答は誤りです。

スマーフ攻撃 - 設定が混在したネットワークデバイスが、ネットワークのブロードキャストアドレスを介して特定のネットワーク上のすべてのホストにパケットを送信することを許可した場合に発生します。

トラフィック分析とは、通信パターンから情報を推測するために、メッセージを傍受して分析するプロセスです。メッセージが暗号化されていて復号できない場合でも実行可能です。一般的に、観測または傍受 保存されたメッセージの数が多いほど、トラフィックから推測できる情報も多くなります。トラフィック分析は、軍事情報、防諜、生活パターン分析などの分野で実施され、コンピュータセキュリティにおいても重要な課題となっています。

割り込み攻撃 - 割り込み攻撃とは、オペレーティングシステムを呼び出して特定のシステムコールを実行させることで、悪意のある動作が行われる攻撃のことです。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 323ページ

ISC2公式CISSP CBKガイド第3版 493ページ

<http://en.wikipedia.org/wiki/Phishing>

最新問題: 727

IS監査マネージャーは、最近完了した企業災害復旧テストの監査に関する作業書類をレビューしています。IS監査マネージャーは、結論を裏付けるために、次のうちどれを特にレビューすべきでしょうか？

- A. データセンター担当者と監査担当者との面談概要
- B. 他の企業の災害復旧監査に関する過去の監査報告書
- C. 監査で指摘された弱点に関する監査意見を反映した要約メモ
- D. すべての偶発性試験の成功と弱点に関する詳細な証拠

Answer: ([解答を表示する](#))

最新問題: 728

組織の内部ネットワークに対する侵入テストを実施する際、テスト実施者がネットワーク上で検出されないために最も効果的な方法はどれでしょうか？

- A. 既存のファイルサーバーまたはドメインコントローラーのIPアドレスを使用します。
- B. 数分ごとにスキャンを一時停止して、しきい値をリセットします。
- C. 誰もログインしていない夜間にスキャンを実施してください。
- D. 各ツールには異なる特性があるため、複数のスキャンツールを使用してください。

Answer: ([解答を表示する](#))

数分ごとにスキャンを一時停止することで、ネットワークへの過負荷を防ぎ、ネットワーク管理者に警告メッセージが表示される可能性のあるしきい値を超えることを避けることができます。サーバーのIPアドレスを使用すると、アドレス競合が発生し、注

目を集めることになります。営業時間外にスキャンを実行すると、活動を隠すためのトラフィックが少なくなるため、検出される可能性が高くなります。複数のツールを使用すると、いずれかのツールが侵入検知システムに検出される可能性が高くなります。

最新問題: 729

情報システム監査担当者が、退職した従業員のアクセス権を削除する手順が文書化されていないことを発見しました。この発見から生じる最も重大なリスクは何ですか？

- A. アクセス権が適時に削除されない場合があります
- B. 不正アクセスは特定できません
- C. 手順が実際の業務と一致しない場合があります
- D. 人事記録がシステムアクセスと一致しない場合があります

Answer: A ([メッセージを残す](#))

最新問題: 730

機密性、信頼性、データの完全性を求めるインターネットビジネスにとって、以下のうちどれが総合的に最も優れた管理方法でしょうか？

- A. セキュアソケットレイヤー (SSL)
- B. 侵入検知システム (IDS)
- C. 公開鍵基盤 (PKI)
- D. 仮想プライベートネットワーク (VPN)

Answer: ([解答を表示する](#)**)**

PKIは、暗号化、デジタル署名、否認防止制御によって機密性と信頼性を確保できるため、総合的に見て最適な技術と言えるでしょう。SSLは機密性を提供できます。IDSは検出制御です。VPNは機密性と認証（信頼性を提供します）。

最新問題: 731

オンラインバンキングアプリケーションにおいて、以下のうちどれが個人情報盗難から最も効果的に保護できるのでしょうか？

- A. 個人パスワードの暗号化
- B. ユーザーを特定の端末に制限する
- C. 二段階認証
- D. アクセスログの定期的なレビュー

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

二要素認証では、本人確認と権限付与を行うための2つの独立した方法が必要です。

要素には、「パスワードなどの 知っていること」、「トークンなどの 持っているもの」、そして生体認証などの 本人であること」が含まれます。これらの要素のうち2つを要求することで、なりすましをより困難にすることができます。パスワードは推測されたり、破られたりする可能性があります。ユーザーを特定の端末に制限することは、オンラインアプリケーションにとって現実的な代替手段ではありません。アクセスログの定期的な確認は検出制御であり、なりすましを防ぐものではありません。

最新問題: 732

IT監査計画に含めるプロジェクトを選択する際に、IS監査担当者にとって最も有用な情報を提供するのはいずれですか？

- A. プロジェクト憲章
- B. プロジェクト計画
- C. プロジェクト課題ログ
- D. プロジェクト事業計画

Answer: D ([メッセージを残す](#))

プロジェクトビジネスケースとは、予想されるコスト、メリット、リスク、実現可能性に基づいて、プロジェクトを開始する根拠と正当性を記述した文書です。プロジェクトビジネスケースは、IT監査計画に含めるプロジェクトを選択する際に、IS監査担当者にとって最も有用な情報を提供します。なぜなら、IS監査担当者が以下のことを行うのに役立つからです。

プロジェクトの目的、範囲、目標、成果物を理解する

プロジェクトが組織の戦略、ビジョン、目標と整合しているかどうかを評価する

プロジェクトの価値提案と投資収益率を評価する

プロジェクトの主要な利害関係者、スポンサー、および所有者を特定する

プロジェクトに関連する潜在的なリスクと問題点を分析する

* 他の競合プロジェクトと比較し、プロジェクトの優先順位を決定する

その他の選択肢は以下のとおりです。

* A. プロジェクト憲章 :プロジェクト憲章とは、プロジェクトの概要、役割、責任、権限を正式に承認し定義する文書です。プロジェクト憲章は、IT監査計画に含めるプロジェクトを選択する際に、IS監査担当者にとって有用な情報を提供しますが、最も有用な情報ではありません。プロジェクト憲章には、IT監査計画への適合性を評価するために不可欠な、プロジェクトのコスト、メリット、リスク、実現可能性に関する十分な詳細情報が記載されていないためです。

* B. プロジェクト計画 :プロジェクト計画とは、プロジェクトの詳細な範囲、スケジュール、予算、リソース、品質、およびコミュニケーション計画を概説する文書です。プロジェクト計画は、IT監査計画に含めるプロジェクトを選択する際に、IS監査担当者にとって有用な情報を提供しますが、最も有用な情報ではありません。プロジェクト計画には、IT監査計画におけるプロジェクトの妥当性を評価する上で重要な、プロジェクトの根拠、正当性、価値提案、および組織の戦略と目標との整合性に関する十分な情報が含まれていないためです。

* C. プロジェクト課題ログ :プロジェクト課題ログとは、プロジェクトの実行中に発生した課題とその解決方法を記録・追跡する文書です。プロジェクト課題ログは、IT監査計画に含めるプロジェクトを選択する際に、IS監査担当者にとって有用な情報を提供しますが、最も有用な情報ではありません。プロジェクト課題ログには、プロジェクトの目的、目標、メリット、実現可能性に関する十分な情報が含まれていないため、IT監査計画における優先順位を決定する上で重要となります。

最新問題: 733

フォローアップを計画する際、IS監査担当者は、最近の組織変更により以前に特定されたリスクが解消されたため、アクションプランの実施は不要になったと運用管理部門から通知を受けました。監査担当者は次に何をすべきでしょうか？

- A. 経営陣の主張を受け入れ、リスクは対処済みであると報告する。
- B. 変更により、リスクが対処されたかどうかを判断することが非現実的になったと報告する。
- C. 変更点を確認し、リスクが対処されているかどうかを判断する。
- D. 変更によって対処が必要な新たなリスクが生じたかどうかを判断する。

Answer: ([解答を表示する](#)**)**

最新問題: 734

TCP/IPモデルにおけるLANまたはWANインターフェース層のデータのプロトコルデータユニット (PDU)は次のうちどれですか？

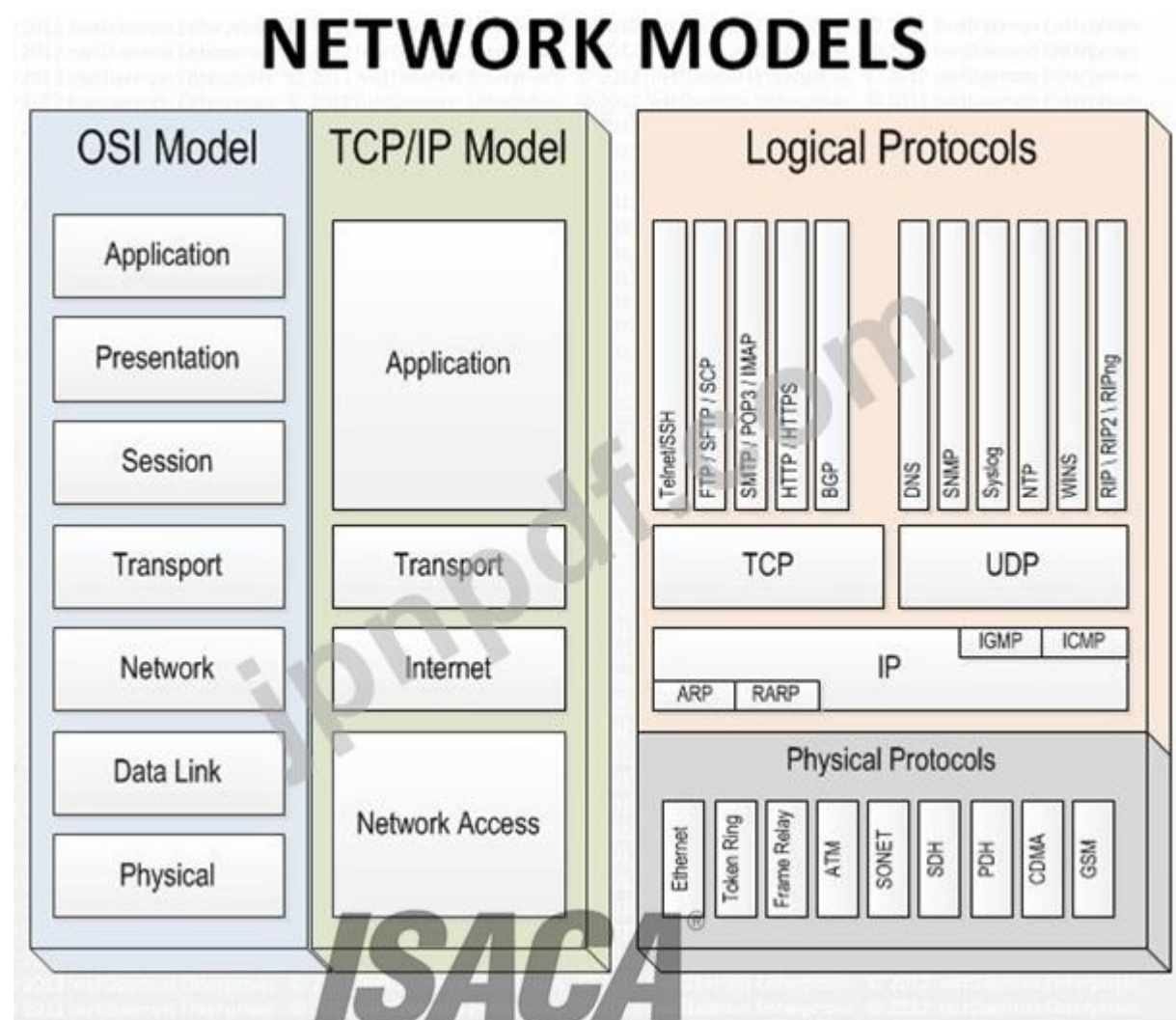
- A. データ
- B. セグメント
- C. パケット
- D. フレームとビット

Answer: D (メッセージを残す)

説明／参考資料：

試験に向けて、TCP/IPモデルに関する以下の情報を知っておく必要があります。

ネットワークモデル



第4層 :アプリケーション層

アプリケーション層は、4層構造のTCP/IPモデルにおいて最上位の層です。アプリケーション層はトランスポート層の上に位置します。アプリケーション層は、TCP/IPアプリケーションプロトコルと、ホストプログラムがネットワークを利用するためにトランスポート層サービスとどのように連携するかを定義します。

アプリケーション層には、DNS (ドメイン命名システム)、HTTP (ハイパーテキスト転送プロトコル)、Telnet、SSH、FTP (ファイル転送プロトコル)、TFTP (簡易ファイル転送プロトコル)、SNMP (簡易ネットワーク管理プロトコル)、SMTP (簡易メール転送プロトコル)、DHCP (動的ホスト構成プロトコル)、X Window、RDP (リモートデスクトッププロトコル)など、上位レベルのプロトコルがすべて含まれます。

レイヤー3. トランスポート層

トランスポート層は、4層構造のTCP/IPモデルにおける第3層です。トランスポート層は、アプリケーション層とインターネット層の間に位置します。トランスポート層の目的は、送信元ホストと宛先ホスト上のデバイスが通信を行えるようにすることです。トランスポート層は、データ転送時に使用される接続のサービスレベルと状態を定義します。

トランスポート層に含まれる主なプロトコルは、TCP（伝送制御プロトコル）とUDP（ユーザーデータグラムプロトコル）です。

レイヤー2. インターネット層

インターネット層は、4層構造のTCP/IPモデルにおける第2層です。インターネット層は、ネットワークアクセス層とトランスポート層の間に位置します。インターネット層は、IPデータグラムと呼ばれるデータパケットにデータを圧縮します。IPデータグラムには、送信元アドレスと宛先アドレス（論理アドレスまたはIPアドレス）の情報が含まれており、ホスト間およびネットワーク間でデータグラムを転送するために使用されます。インターネット層は、IPデータグラムのルーティングも担当します。

パケット交換ネットワークは、コネクションレス型のインターネットワーク層に依存しています。この層はインターネット層と呼ばれ、ホストが任意のネットワークにパケットを挿入し、宛先まで独立して配信できるようにする役割を担っています。宛先側では、データパケットは送信時とは異なる順序で到着する場合があります。上位層は、これらのパケットを適切なネットワークアプリケーション（アプリケーション層で動作）に配信するために、順序を並べ替える役割を担います。

インターネット層に含まれる主なプロトコルは、IP（インターネットプロトコル）、ICMP（インターネット制御メッセージプロトコル）、ARP（アドレス解決プロトコル）、RARP（逆アドレス解決プロトコル）、およびIGMP（インターネットグループ管理プロトコル）です。

レイヤー1. ネットワークアクセスレイヤー

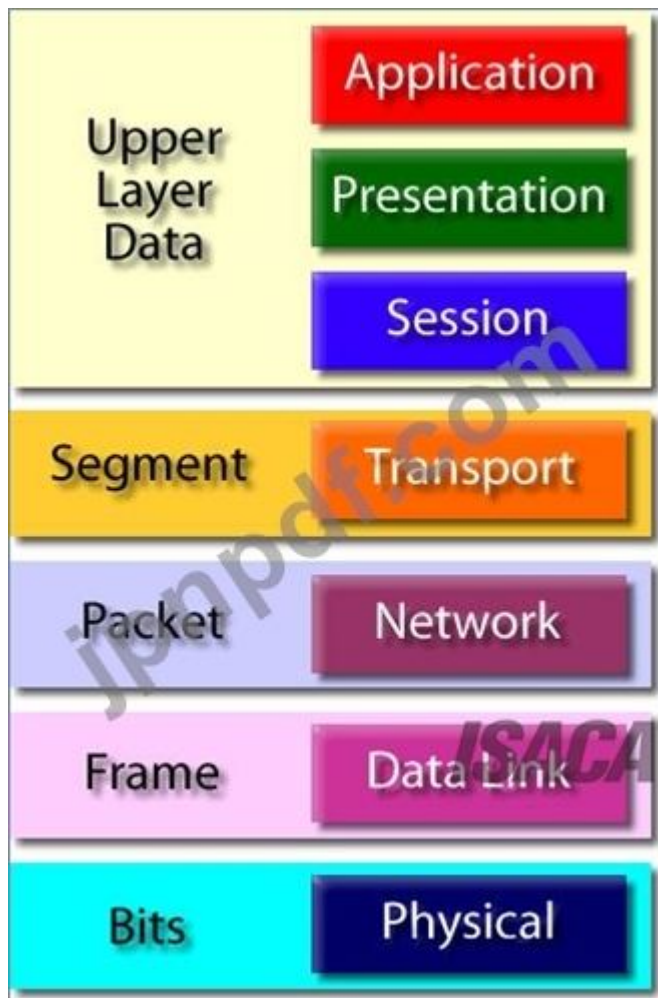
ネットワークアクセス層は、4層構造のTCP/IPモデルの最初の層です。ネットワークアクセス層は、データがネットワークを介して物理的に送信される方法の詳細を定義します。これには、同軸ケーブル、光ファイバー、ツイストペア銅線などのネットワーク媒体と直接接続するハードウェアデバイスによって、ビットが電氣的または光学的にどのように信号化されるかが含まれます。ネットワークアクセス層に含まれるプロトコルには、イーサネット、トークンリング、FDDI、X.25、フレームリレーなどがあります。

上記に挙げたLANアーキテクチャの中で最も一般的なのはイーサネットです。イーサネットは、共有メディアで動作する場合、CSMA/CD（キャリアセンス多重アクセス/衝突検出）と呼ばれるアクセス方式を使用してメディアにアクセスします。アクセス方式は、ホストがメディア上にデータを配置する方法を決定します。

CSMA/CDアクセス方式では、すべてのホストが媒体に平等にアクセスでき、ネットワークトラフィックがないときにデータを送信できます。ホストがデータを送信しようとする、他のホストが既に媒体を使用しているかどうかを確認します。媒体にトラフィックがある場合は、ホストは待機し、トラフィックがない場合は、データを媒体に送信します。しかし、2つのシステムが同時に媒体にデータを送信しようとする、衝突が発生し、データが破壊されます。送信中にデータが破壊された場合は、データを再送信する必要があります。衝突後、各ホストは短い時間待機し、その後、データが再送信されます。

プロトコルデータユニット（PDU）：

プロトコルデータユニット - PDU



以下の回答は誤りです。

データ - アプリケーション層データPDU

セグメント - トランスポート層データPDU

パケット - ネットワークインターフェース層データ PDU

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版、272ページ

最新問題: 735

Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

- A. Pilot
- B. Paper
- C. Unit
- D. System

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

A paper test is appropriate for testing a BCP. it is a walkthrough of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster.

Choices A, C and D are not appropriate for a BCP.

最新問題: 736

An IS auditor is assigned to review the IS department's quality procedures. Upon contacting the IS manager, the auditor finds that there is an informal unwritten set of standards. Which of the following should be the auditor's NEXT action?

- A. Make recommendations to IS management as to appropriate quality standards
- B. Postpone the audit until IS management implements written standards
- C. Document and test compliance with the informal standards
- D. Finalize the audit and report the finding

Answer: C ([メッセージを残す](#))

Explanation

The auditor's next action after finding that there is an informal unwritten set of standards in the IS department is to document and test compliance with the informal standards. This is because the auditor's role is to evaluate the adequacy and effectiveness of the existing controls, regardless of whether they are formal or informal, written or unwritten. The auditor should also assess the risks and implications of having informal standards, such as lack of consistency, accountability, or traceability. The auditor should not make recommendations, postpone the audit, or finalize the audit without performing the audit procedures.

References:

CISA Review Manual (Digital Version), Chapter 2, Section 2.21

CISA Online Review Course, Domain 1, Module 1, Lesson 12

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 737

金融機関における海外送金取引に適用された誤った為替レートを、IS監査人が検出するのに最も適した方法はどれですか？

- A. 教師あり機械学習技術を用いて、誤った入力を予測する回帰モデルを開発する
- B. 毎日終業時に継続的な監査スクリプトを実行する
- C. 取引監査におけるコンピュータ支援監査技術 (CAAT)の開発
- D. 各日の終わりに処理された取引に対してサンプリングテストを実施する

Answer: C ([メッセージを残す](#))

最新問題: 738

Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

- A. Inability to utilize the site when required
- B. Inability to test the recovery plans onsite
- C. Equipment compatibility issues at the site
- D. Mismatched organizational security policies

Answer: A ([メッセージを残す](#))

Explanation

The greatest risk of using a reciprocal site for disaster recovery is the inability to utilize the site when required. A reciprocal site is an agreement between two organizations to provide backup facilities for each other in case of a disaster. However, this arrangement may not be reliable or enforceable, especially if both organizations are affected by the same disaster or have conflicting priorities. Therefore, the IS auditor should recommend that management consider alternative options for disaster recovery, such as dedicated sites or cloud services¹². References:

CISA Review Manual, 27th Edition, page 3381

CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

最新問題: 739

When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

- A. Before transaction completion
- B. Immediately after an EFT is initiated
- C. During run-to-run total testing
- D. Before an EFT is initiated

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

An application-level edit check to verify availability of funds should be completed at the electronic funds transfer (EFT) interface before an EFT is initiated.

最新問題: 740

An employee who denies accusations of sending inappropriate images to other employees has been discharged. For evidential purposes, the mail database for the discharged employee's computer should be:

- A. deleted as it could subject the organization to further legal liability
- B. impounded by physically removing the disk drive
- C. backed up to the server, where its access can be tightly restricted
- D. copied to write-once, read-many media using the computer's OS tools

Answer: C ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 741

新しいアプリケーションには複数のインターフェースが必要になります。開発ライフサイクルの早い段階でインターフェースのエラーを検出するために使用できるテスト方法は次のうちどれですか？

- A. 受容
- B. 上から下へ
- C. 社交性
- D. ボトムアップ

Answer: ([解答を表示する](#))

最新問題: 742

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- A. True
- B. False

Answer: [\(解答を表示する\)](#)

Explanation/Reference:

Database snapshots can provide an excellent audit trail for an IS auditor.

最新問題: 743

An IS auditor is reviewing a machine learning model that predicts the likelihood that a user will watch a certain movie. Which of the following would be of GREATEST concern to the auditor?

- A. The data set for training the model was obtained from an unreliable source
- B. When the model was tested with data drawn from a different population, the accuracy decreased
- C. An open source programming language was used to develop the model
- D. The model was tested with data drawn from the same population as the training data

Answer: A ([メッセージを残す](#))

The quality and reliability of the training data are crucial for the model's accuracy and overall performance. If the training data comes from an unreliable source, the model's predictions could be biased, inaccurate, or unreliable, leading to poor outcomes when applied to real-world scenarios. Ensuring the integrity, quality, and reliability of the training data is fundamental for any machine learning model.

While decreased accuracy when tested with data from a different population, the use of open- source programming languages, and testing with data from the same population are important factors to consider, the reliability of the training data is the most critical issue because it directly affects the model's ability to learn correctly and generalize to new data.

最新問題: 744

A global organization's policy states that all workstations must be scanned for malware each day. Which of the following would provide an IS auditor with the BEST evidence of continuous compliance with this policy?

- A. Penetration testing results
- B. Management attestation
- C. Anti-malware tool audit logs
- D. Recent malware scan reports

Answer: C ([メッセージを残す](#))

Anti-malware tool audit logs would provide an IS auditor with the best evidence of continuous compliance with the global organization's policy that states that all workstations must be scanned for malware each day. Anti-malware tool audit logs are records that capture the activities and events related to the anti-malware software installed on the workstations, such as scan schedules, scan results, updates, alerts, and actions taken¹. These logs can help the IS auditor to verify that the anti-malware software is functioning properly, that the scans are performed regularly and effectively, and that any malware incidents are detected and resolved in a timely manner². Anti-malware tool audit logs can also help the IS auditor to identify any gaps or weaknesses in the anti-malware policy or implementation, and to provide recommendations for improvement³.

The other options are not the best evidence of continuous compliance with the anti-malware policy. Penetration testing results are reports that show the vulnerabilities and risks of the workstations and network from an external or internal attacker's perspective⁴. While penetration testing can help to assess the security posture and resilience of the organization, it does not

provide information on the daily anti-malware scans or their outcomes. Management attestation is a statement or declaration from the management that they have complied with the anti-malware policy⁵. While management attestation can demonstrate commitment and accountability, it does not provide objective or verifiable evidence of compliance. Recent malware scan reports are documents that show the summary or details of the latest anti-malware scans performed on the workstations. While recent malware scan reports can indicate the current status and performance of the anti-malware software, they do not provide historical or comprehensive evidence of compliance.

References:

- * Malwarebytes Anti-Malware (MBAM) log collection and threat reports ...
- * Malicious Behavior Detection using Windows Audit Logs
- * PCI Requirement 5.2 - Ensure all Anti-Virus Mechanisms are Current ...
- * Management Attestation - an overview | ScienceDirect Topics
- * How to Read a Malware Scan Report | Techwalla

最新問題: 745

Which of the following is the BEST method for uncovering shadow IT within an organization?

- A. Analyze help desk tickets.
- B. Review secondary approval thresholds.
- C. Use a cloud access security broker (CASB).
- D. Review business processes.

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

最新問題: 746

A finance department has a multi-year project to upgrade the enterprise resource planning (ERP) system hosting the general ledger. and in year one, the system version upgrade will be applied. Which of the following should be the PRIMARY focus of the IS auditor reviewing the first year of the project?

- A. unit testing
- B. Network performance
- C. User acceptance testing (UAT)
- D. Regression testing

Answer: D ([メッセージを残す](#))

The primary focus of the IS auditor reviewing the first year of the project should be regression testing.

Regression testing is a type of testing that ensures that the existing functionality of the system is not affected by the changes or upgrades made to the system. Since the project involves upgrading the ERP system hosting the general ledger, which is a critical and complex component of the finance department, it is important to verify that the upgrade does not introduce any errors or defects that could compromise the accuracy, completeness, and reliability of the financial data and reports. Regression testing can help identify and resolve any issues before they affect the users and the business processes.

Unit testing, network performance, and user acceptance testing (UAT) are also important aspects of the project, but they are not the primary focus of the IS auditor in the first year. Unit testing is a type of testing that verifies that each individual module or component of the system works as expected. Network performance is a measure of how well the system can communicate and exchange data with other systems and devices over a network. User acceptance testing (UAT) is a type of testing that validates

that the system meets the user requirements and expectations. These aspects are more relevant in later stages of the project, when the system is more developed and ready for deployment.

References:

ERP Upgrade: The Path to Modernization | SAP

ERP System Validation: Your Guide To Successfully Validating ERP Systems The role of internal auditors in ERP#based organizations What is Regression Testing? Definition, Tools and Examples What is Unit Testing? Definition, Tools and Examples What is Network Performance? Definition, Metrics and Examples What is User Acceptance Testing (UAT)? Definition, Process and Examples

最新問題: 747

Which of the following security measures is MOST important for protecting Internet of Things (IoT) devices from potential cyberattacks?

- A. Confirming firmware compliance to current security requirements
- B. Reviewing and updating the network diagram on a regular basis
- C. Changing default passwords
- D. Logging and monitoring network traffic

Answer: C ([メッセージを残す](#))

The most important security measure for protecting Internet of Things (IoT) devices from potential cyberattacks is changing default passwords. Many IoT devices come with default, easily guessable passwords, which are a common target for attackers. Changing these passwords to strong, unique ones significantly reduces the risk of unauthorized access and helps secure the devices from cyberattacks.

最新問題: 748

While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered.

Which of the following control is implemented by Lily?

- A. Range Check
- B. Duplicate Check
- C. Existence check
- D. Reasonableness check

Answer: B ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

Explanation/Reference:

In a duplicate check control new transaction are matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check - The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US \$ 4000. If a check exceeds US \$ 4000, data would be rejected for further verification/authorization.

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check - Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups - Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerized table that matches a code to a city name.

Existence Check - Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit - a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check - a field should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. This is identified as a key in field and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check - if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his/her date of birth.

The following were incorrect answers:

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check - Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check - Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 215

最新問題: 749

The PRIMARY purpose of a configuration management system is to:

- A. track software updates.
- B. define baselines for software.
- C. support the release procedure.
- D. standardize change approval.

Answer: ([解答を表示する](#))

Explanation

A configuration management system is a process that establishes and maintains the consistency of a product's attributes throughout its life cycle. It helps to identify and control the functional and physical characteristics of a product, and to record and report any changes to those characteristics. A configuration management system also supports the audit of the product to verify its conformance to requirements.

構成管理システムの主要な活動の一つは、ソフトウェアのベースラインを定義することです。ベースラインとは、比較や測定の基準となる固定された参照点です。要件、設計文書、テスト計画、ソフトウェアコンポーネントなど、あらゆる構成項目に対してベースラインを設定できます。ベースラインを設定することで、ソフトウェア製品が本来の目的と品質基準を満たしていること、そしてソフトウェアへの変更が適切に管理され、文書化されることを保証できます。

構成管理システムは、ソフトウェアの更新の追跡、リリース手順のサポート、変更承認の標準化など、その他の活動もサポートしますが、これらはその主な目的ではありません。

したがって、他の選択肢は誤りです。

参考文献 :: 構成管理とは - Red Hat : 構成管理 | 定義、重要性、および利点 - ServerWatch

最新問題: 750

A disaster recovery plan (DRP) should include steps for:

- A. assessing and quantifying risk.
- B. negotiating contracts with disaster planning consultants.
- C. identifying application control requirements.
- D. obtaining replacement supplies.

Answer: D ([メッセージを残す](#))

A disaster recovery plan (DRP) is a set of detailed, documented guidelines that outline a business' critical assets and explain how the organization will respond to unplanned incidents. Unplanned incidents or disasters typically include cyberattacks, system failures, power outages, natural disasters, equipment failures, or infrastructure damage¹. A DRP aims to minimize the impact of a disaster on the business continuity, data integrity, and service delivery of the organization. A DRP also helps the organization recover from a disaster as quickly and efficiently as possible.

A DRP should include steps for obtaining replacement supplies, as this is an essential part of restoring the normal operation of the organization after a disaster. Replacement supplies may include hardware, software, data, network components, office equipment, or other resources that are needed to resume the business functions and processes that were disrupted by the disaster. Obtaining replacement supplies may involve contacting vendors, suppliers, or partners; activating backup or alternative systems; or purchasing or renting new equipment. A DRP should identify the sources, locations, and costs of the replacement supplies, as well as the procedures and responsibilities for acquiring and installing them.

他の 3 つのオプションは、災害前の計画プロセスの一部であるか、災害復旧の目的に直接関係しないため、DRP に含めるべき手順ではありません。リスクの評価と定量化は、組織に影響を与える可能性のある潜在的な脅威と脆弱性を特定し、各シナリオの可能性と影響を判断するのに役立つため、DRP を作成する前に実行すべき手順です 2。災害計画コンサルタントとの契約交渉も、外部の専門知識とガイダンスを使用して組織が DRP を設計、実装、テスト、および維持するのに役立つ災害前の活動です 3。アプリケーション制御要件の特定は、DRP の手順ではなく、組織が使用するソフトウェア アプリケーションの品質、セキュリティ、および信頼性を保証するアプリケーション開発および保守プロセスの一部です。したがって、代替品を入手することが正しい解決策です。

参考文献：

- * 災害復旧計画とは？ + チェックリスト
- * リスク評価 - ISACA
- * 災害復旧計画 - ISACA
- * [アプリケーション制御 - ISACA]

最新問題: 751

"Nowadays, computer security comprises mainly "preventive"" measures."

- A. True
- B. True only for trusted networks
- C. True only for untrusted networks
- D. False
- E. None of the choices.

Answer: ([解答を表示する](#))

Section: Protection of Information Assets

Explanation:

"Nowadays, computer security comprises mainly ""preventive"" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network and is normally implemented as software running on the machine or as physical integrated hardware."

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 752

データ所有者がデータに誤った分類レベルを割り当てた場合、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？

- A. データを適切に保護するための管理措置が適用されていない可能性があります。
- B. システム管理者によってデータが暗号化されていない可能性があります。
- C. 競合他社がデータを閲覧できる可能性があります。
- D. 管理コストがIT資産の本来の価値を超える可能性があります。

Answer: A (メッセージを残す)

正解はAです。データ所有者がデータに誤った分類レベルを割り当てた場合、IS監査担当者にとって最大の懸念事項は、データを適切に保護するための管理策が適用されない可能性があることです。データ分類とは、データの機密性やビジネスへの影響に基づいてデータ資産进行分类するプロセスです。データ分類は、組織がデータの価値とリスクに応じてデータを識別、保護、管理するのに役立ちます。データ所有者とは、データへのアクセスと使用を定義、分類、管理する権限と責任を持つ個人または組織のことです。

データ分類とは、通常、データ資産に「公開」「内部」「機密」「制限付き」などのラベルやタグを割り当てることを指します。これらのラベルは、データに必要な保護レベルと取り扱いレベルを示します。

組織のデータ分類に基づき、暗号化、アクセス制御リスト、監査ログ、バックアップポリシーなど、データを保護するための適切な制御策を実施することができます。これらの制御策は、データの不正アクセス、漏洩、改ざん、損失を防ぎ、関連法規の遵守を確保するのに役立ちます。

データ所有者がデータに誤った分類レベルを割り当てると、データの保護不足または過剰保護につながる可能性があります。保護不足とは、データが本来あるべきレベルよりも低いレベルで分類されることを意味し、データが侵害または漏洩するリスクが高まります。たとえば、データ所有者が個人健康情報 (PHI) を機密ではなく公開として分類した場合、適切な許可や同意なしに誰でもデータにアクセスしたり共有したりできる可能性があります。これは、データ主体のプライバシー権や、HIPAA (医療保険の携行性と説明責任に関する法律) などの規制のコンプライアンス要件に違反する可能性があります。過剰保護とは、データが本来あるべきレベルよりも高いレベルで分類されることを意味し、データの可用性や利用可能性が制限されます。たとえば、データ所有者がマーケティング資料を公開ではなく制限付きとして分類した場合、潜在的な顧客やパートナーがデータにアクセスしたり閲覧したりできなくなる可能性があります。これは、データのビジネス価値と機会を低下させる可能性があります。

したがって、IS監査人は、データ所有者によるデータ分類の正確性と一貫性について懸念すべきである。なぜなら、それはデータ管理のセキュリティと効率性に影響を与えるからである。IS監査人は、データ分類に関するポリシーと手順をレビューし、データ所有者がデータを分類するための十分な知識とスキルを有していることを確認し、データ分類ラベルがデータの実際の機密性および影響と一致していることをテストする必要がある。

参考文献：

- * データ分類 :その内容と実装方法
- * データ分類とは？ - 定義、レベル、例...
- * データ分類 :データセキュリティリーダーのためのガイド

最新問題: 753

Which of the following would be MOST helpful in ensuring security procedures are followed by employees in a multinational organization?

- A. Security architecture review
- B. Regular clean desk reviews

- C. Comprehensive end-user training
- D. Regular policy updates by management

Answer: C ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: **754**

IS監査人が組織のデータ損失防止 (DLP) 対策の運用効果を評価する上で、最も信頼性の高い方法は次のうちどれですか？

- A. インタビューを実施して、データ保護上の潜在的な脆弱性を特定する。
- B. すべてのコンピュータシステムに最新のDLPソフトウェアがインストールされていることを確認してください。
- C. 業界のベストプラクティスに基づいてデータ分類レベルを見直します。
- D. 機密ファイルが個人のUSBデバイスに送信されないことを確認してください。

Answer: B ([メッセージを残す](#))

最新問題: **755**

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- A. Check digit
- B. Existence check
- C. Completeness check
- D. Reasonableness check

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks.

最新問題: **756**

A financial institution suspects that a manager has been crediting customer accounts without authorization.

Which of the following is the MOST effective method to validate this concern?

- A. Attribute sampling
- B. Stop or go sampling
- C. Variable sampling
- D. Discovery sampling

Answer: A ([メッセージを残す](#))

最新問題: **757**

An IS auditor is evaluating the risk associated with moving from one database management system (DBMS) to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

- A. Preserving the same data inputs
- B. Preserving the same data structure
- C. Preserving the same data interfaces

D. Preserving the same data classifications

Answer: A ([メッセージを残す](#))

最新問題: 758

IS監査担当者が継続的監視システムを導入する際に推奨される最初のステップは何ですか？

- A. 既存の内部統制を文書化する
- B. 内部統制のコンプライアンステストを実施する
- C. 管理監視運営委員会を設置する
- D. 組織内の高リスク領域を特定する

Answer: D ([メッセージを残す](#))

継続的監視システムを導入する際、IS監査担当者が最初に行うべきことは、組織内の高リスク領域を特定することである。

最新問題: 759

Which of the following should be the PRIMARY objective of a migration audit?

- A. System performance
- B. Data integrity
- C. Control adequacy
- D. Business continuity

Answer: B ([メッセージを残す](#))

最新問題: 760

Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

- A. DTE
- B. DCE
- C. DME
- D. DLE

Answer: (解答を表示する)

Explanation/Reference:

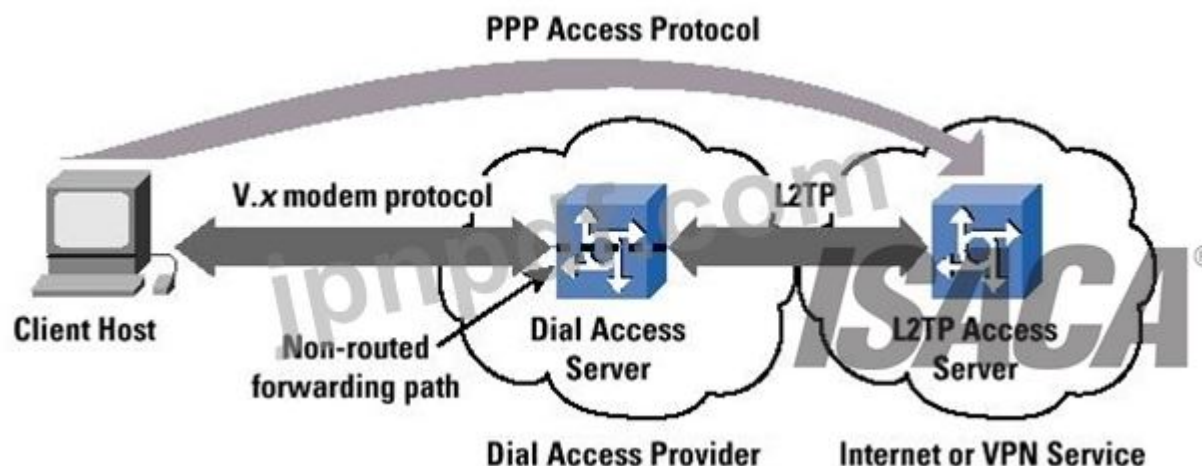
Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

For your exam you should know below information about WAN Technologies:

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation. PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.



Point-to-point protocol

X.25

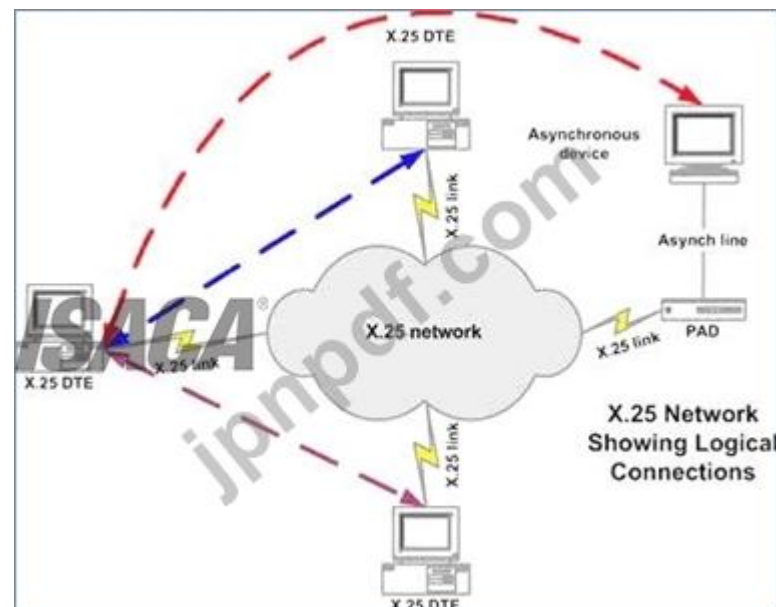
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

X.25



Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Two main types of equipments are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality.

Frame relay is any to any service.

Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium

ISDN



Asynchronous Transfer Mode (ATM)

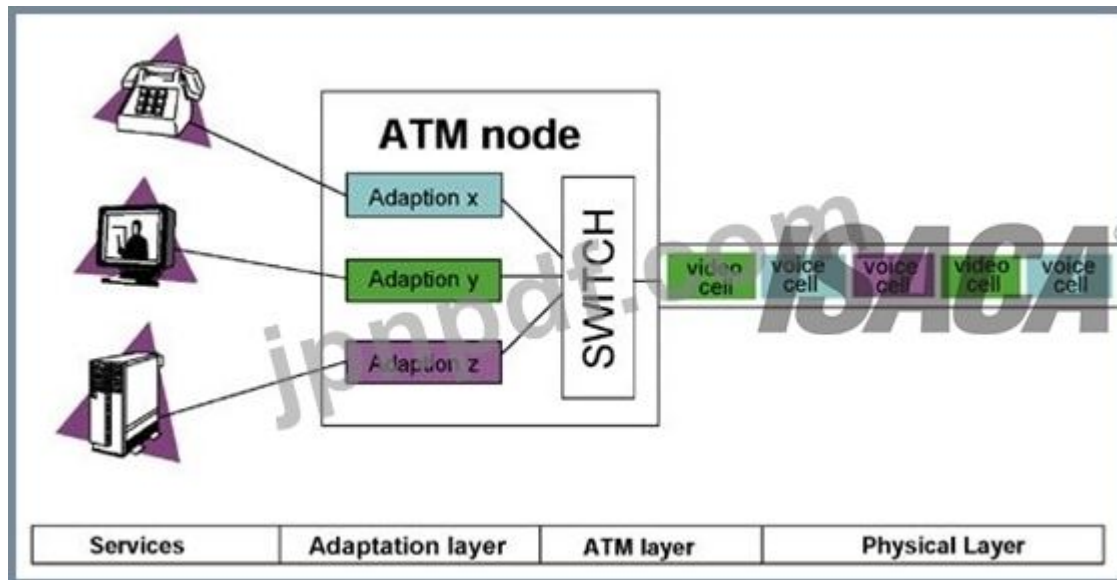
Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM

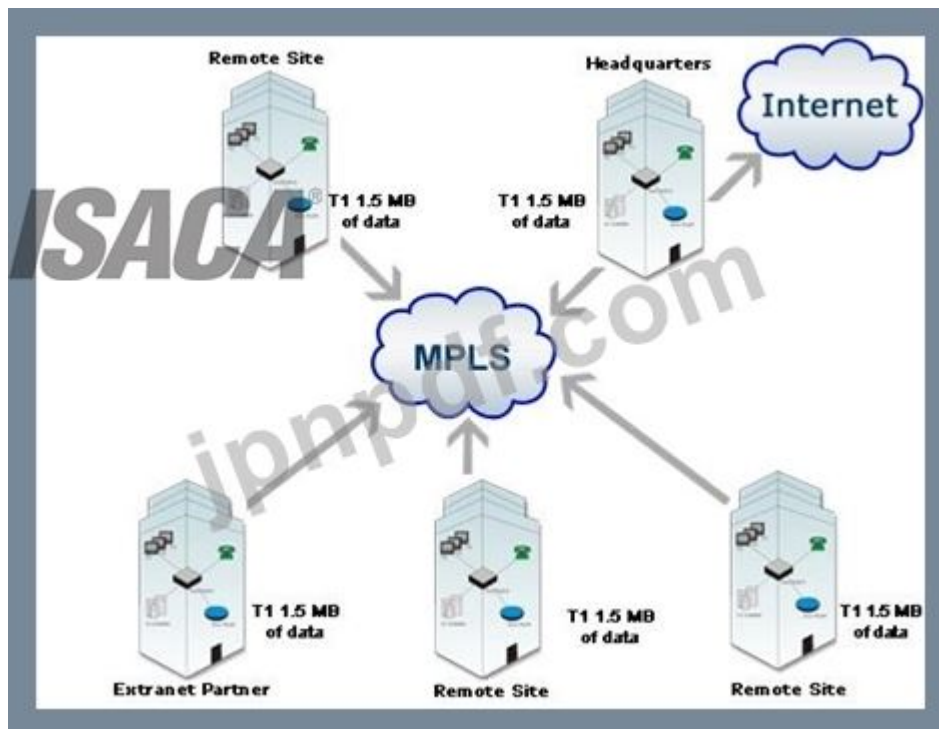
Asynchronous Transfer Mode



Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

DTE - Data Terminal Equipment (DTE) is usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

DME - Not a valid frame relay technique

DLE - Not a valid frame relay technique

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

最新問題: 761

In which phase of the audit life cycle process should an IS auditor initially discuss observations with management?

A. Planning phase

B. Reporting phase

C. Follow-up phase

D. Fieldwork phase

Answer: ([解答を表示する](#))

Comprehensive and Detailed Step-by-Step Explanation:

Audit findings should be communicated as early as possible to avoid misunderstandings, provide an opportunity for corrective action, and ensure transparency.

* Option A (Incorrect):The planning phase involves defining audit scope, objectives, and methodology, but findings are not yet available to discuss with management.

* Option B (Incorrect):The reporting phase formalizes audit results, but discussing issuesonlyat this stage may lead to delays in corrective action.

* Option C (Incorrect):The follow-up phase ensures that management has implemented corrective actions, but this occursafterthe initial discussion of findings.

* Option D (Correct):The fieldwork phase is when auditors activelygather evidence, analyze data, and identify issues. Discussing observationsduringthis phase allows for immediate clarification, validation, and resolution of misunderstandings before the final report.

Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Discusses audit engagement, reporting, and communication best practices.

最新問題: 762

IS監査人が監査において重要性の概念を適用することが最も重要なのはどのような場合でしょうか？

A. 監査業務を計画する際

B. 現地調査のための情報収集時

C. 規制要件違反が確認された場合

D. 被監査者からの陳述を評価する際

Answer: A ([メッセージを残す](#))

重要性の概念は、情報システム監査人が監査業務を計画する際に適用すべき最も重要な概念です。なぜなら、重要性の概念は、監査人が監査の範囲、目的、手順、およびリソースを決定するのに役立つからです。

重要性とは、情報の省略または誤記が利用者の意思決定や監査目標の達成に及ぼす影響の度合いを指します。重要性の概念を適用することで、監査人は監査の最も重要かつ関連性の高い領域に集中し、些細な事項や重要でない事項に時間と労力を浪費することを避けることができます。他の選択肢は、監査業務の計画ほど重要ではありません。なぜなら、それらは計画段階で行われる重要性評価に基づいているか、または影響を受けるからです。参考文献：

* ISACA、CISAレビューマニュアル、第27版、第1章、セクション1.31

* ISACA、IT監査および保証基準、IS監査および保証専門家向けガイドラインおよびツールとテクニック、セクション12022

最新問題: 763

Which of the following is the BEST approach to validate whether a streaming site can continue to provide service during a period of live streaming with an anticipated high volume of viewers?

- A. Fuzzing
- B. Usability test
- C. Fault grading
- D. Load test

Answer: D ([メッセージを残す](#))

<https://testlio.com/blog/live-stream-best-practices/>

最新問題: 764

When testing the adequacy of tape backup procedures which step BEST verifies that regularly scheduled backups are timely and run to completion?

- A. Observing the execution of a daily backup run
- B. Reviewing a sample of system-generated backup logs
- C. Evaluating the backup policies and procedures
- D. interviewing key personnel involved in the backup process

Answer: ([解答を表示する](#))

最新問題: 765

.Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem? Choose the BEST answer.

- A. Expert systems
- B. Neural networks
- C. Integrated synchronized systems
- D. Multitasking applications

Answer: ([解答を表示する](#))

Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

最新問題: 766

Which of the following is MOST critical to the success of an information security program?

- A. Management's commitment to information security
- B. User accountability for information security
- C. Alignment of information security with IT objectives
- D. Integration of business and information security

Answer: A ([メッセージを残す](#))

The most critical factor for the success of an information security program is management's commitment to information security. Management's commitment to information security means that the senior management supports, sponsors, funds, monitors and enforces the information security program within the organization.

Management's commitment to information security also demonstrates leadership, sets the tone and culture, and establishes the strategic direction and objectives for information security. User accountability for information security, alignment of information security with IT objectives, and integration of business and information security are also important factors for the success of an information security program, but they are not as critical as management's commitment to information security, as they depend on or derive from it.

References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **767**

IS監査担当者が、買掛金システムのリスクに対して統制をマッピングしています。システムのエラーを検出するための最適な統制は何ですか？

- A. 業務目標に沿ったプロセスの構築
- B. 新規支払いの品質管理レビュー
- C. 支払いの管理承認
- D. 入力検証

Answer: ([解答を表示する](#))

セクション: 情報システムの監査プロセス

最新問題: **768**

Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

- A. Unauthorized access from outside the organization
- B. Unauthorized access from within the organization
- C. A delay in Internet connectivity
- D. A delay in downloading using File Transfer Protocol (FTP)

Answer: ([解答を表示する](#))

Firewalls are meant to prevent outsiders from gaining access to an organization's computer systems through the internet gateway. They form a barrier with the outside world, but are not intended to address access by internal users; they are more likely to cause delays than address such concerns.

最新問題: **769**

暗号化されたデータにアクセスし、その情報を収集しようとする犯人

ネットワーク経由で送信される場合は、以下を使用します。

- A. 盗聴。
- B. なりすまし。
- C. 交通分析。
- D. 仮装。

Answer: [\(解答を表示する\)](#)

In traffic analysis, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, and the intruder is able to guess the type of communication taking place. This typically is used when messages are encrypted and eavesdropping would not yield any meaningful results, in eavesdropping, which also is a passive attack, the intruder gathers the information flowing through the network with the intent of acquiring and releasing message contents for personal analysis or for third parties. Spoofing and masquerading are active attacks, in spoofing, a user receives an e-mail that appears to have originated from one source when it actually was sent from another source. In masquerading, the intruder presents an identity other than the original identity.

最新問題: 770

監査報告書に重要な調査結果を含めるかどうかの最終決定は、以下の者が行うべきである。

- A. 監査委員会
- B. 被監査企業のマネージャー。
- C. IS監査員。
- D. 組織のCEO

Answer: C ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

IS監査担当者は、監査報告書に含めるか除外するかについて最終的な決定を下すべきである。他の選択肢では、監査人の独立性が制限されるだろう。

最新問題: 771

企業ネットワークに導入する前に、新しいデバイスを強化する主な理由は何ですか？

- A. 組織の規則を遵守するため
- B. 機器のメンテナンスを容易にするため
- C. 攻撃への曝露を減らす
- D. ソフトウェアライセンスの競合を避けるため

Answer: C ([メッセージを残す](#))

セクション: 情報システムの運用、保守およびサポート

最新問題: 772

属性サンプリングを利用する場合、次のうちどれがサンプルサイズを増加させる原因となりますか？

- A. 予想されるエラー率の低下
- B. 人口減少
- C. 許容可能なエラー率の低下

D. 許容リスクレベルの上昇

Answer: A ([メッセージを残す](#))

最新問題: 773

適切なファイアウォールポリシーを作成するための最初のステップは何ですか？

- A. 最小権限の原則に従ってユーザーにアクセス権を割り当てる
- B. 適切なファイアウォールハードウェアとソフトウェアの選定
- C. メール、ウェブ、FTPサーバーなどのネットワークアプリケーションを識別する
- D. ファイアウォールアクセスルールの設定

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

外部からアクセスされる可能性のあるメールサーバー、ウェブサーバー、FTPサーバーなどのネットワークアプリケーションを特定することは、適切なファイアウォールポリシーを作成するための最初のステップです。

最新問題: 774

データセンターの監査において、IS監査担当者が物理セキュリティ管理を理解するための最良の方法は次のとおりです。

- A. 施設内を見学し、物理的なセキュリティ対策を確認する。
- B. 建物の設計図を入手し、侵入箇所を特定する。
- C. データセンターの物理的なセキュリティ手順を見直す。
- D. 警報機器ベンダーに連絡し、データセンター内のどこに警報機器が設置されているかを確認してください。

Answer: A ([メッセージを残す](#))

最新問題: 775

監査対象企業の事業計画のレビューは、組織のIT戦略計画のレビューと比較して、いつ実施すべきでしょうか？

- A. 監査クライアントの事業計画をレビューすることは、組織のIT戦略計画をレビューする前に行うべきです。
- B. 監査クライアントの事業計画のレビューは、組織のIT戦略計画のレビューの後に行うべきである。
- C. 監査クライアントの事業計画のレビューは、組織のIT戦略計画のレビュー中に実施する必要があります。
- D. 監査クライアントの事業計画のレビューは、組織のIT戦略計画とは無関係に行うべきである。

Answer: A ([メッセージを残す](#))

監査対象企業の事業計画をレビューすることは、組織のIT戦略計画をレビューする前に実施すべきである。

最新問題: 776

The PRIMARY reason to perform internal quality assurance (QA) for an internal audit function is to ensure:

- A. Internal audit activity conforms with audit standards and methodology.
- B. The audit function is adequately governed and meets performance metrics.
- C. Inherent risk in audits is minimized.
- D. Audit resources are used most effectively.

Answer: A ([メッセージを残す](#))

Internal quality assurance (QA) reviews are conducted to ensure conformance with professional audit standards and methodology.

Option A (Correct):The primary purpose of QA reviews is to confirm that the internal audit function adheres to industry standards, such as ISACA's IT audit framework and the International Standards for the Professional Practice of Internal Auditing (IPPF).

Option B (Incorrect):While governance and performance metrics are important, conformance to standards is the primary goal of QA reviews.

Option C (Incorrect):Risk management is part of audits, but QA reviews focus on adherence to methodology rather than reducing audit risk.

Option D (Incorrect):Efficient resource usage is a goal but not the main objective of an audit QA program.

Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Covers audit quality assurance and compliance with professional standards.

最新問題: 777

事業継続管理ライフサイクルにおいて、以下のうちどれが最も早い段階で行われるべきでしょうか？

- A. 事業継続手順の定義
- B. 重要なビジネスプロセスの特定
- C. 研修および啓発プログラムの開発
- D. 脅威とリスクの評価を実施する

Answer: D ([メッセージを残す](#))

セクション：情報資産の保護

最新問題: 778

顧客データの保護を目的とした、特定の情報セキュリティ対策を義務付ける新たな規制が制定されました。情報セキュリティ監査人がこの規制に照らして監査を行う際に、最も役立つのは次のうちどれでしょうか？

- A. コンプライアンスギャップ分析
- B. 顧客データ保護における役割と責任
- C. 顧客データフロー図
- D. 新規制への適応に関するベンチマーク調査

Answer: ([解答を表示する](#)**)**

コンプライアンスギャップ分析とは、特定の規制や基準に対する組織の現在のコンプライアンス状況を詳細にレビューすることです。これにより、要件を満たしていない領域や管理策を特定し、リスクレベルを評価し、コンプライアンスを達成するために講じることができる是正措置を決定することができます¹²。コンプライアンスギャップ分析は、組織のコンプライアンス状況、ギャップ、および是正計画を明確かつ包括的に示すため、新しい規制に対する監査を行う際にIS監査人がレビューする最も有用なツールです。

参考文献

1：情報セキュリティアーキテクチャ：ギャップ評価と優先順位付け - ISACA

2：コンプライアンスギャップ分析の実施方法 - Sprinto

最新問題: 779

組織のITプロセスを直接収集した証拠から理解する場合と比較して、過去の監査報告書は証拠としてどれほど価値があるのでしょうか？

- A. 同じ値。

- B. より高い価値。
- C. 価値が低い。
- D. 過去の監査報告書は関係ありません。

Answer: C ([メッセージを残す](#))

組織のITプロセスを理解しようとするIS監査人にとって、過去の監査報告書は、直接収集された証拠よりも価値が低いとみなされる。

最新問題: 780

What is often assured through table link verification and reference checks?

- A. Database integrity
- B. Database synchronization
- C. Database normalcy
- D. Database accuracy

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Database integrity is most often ensured through table link verification and reference checks.

最新問題: 781

Which of the following device in Frame Relay WAN technique is generally customer owned device that provides a connectivity between company's own network and the frame relays network?

- A. DTE
- B. DCE
- C. DME
- D. DLE

Answer: A ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

Explanation:

Data Terminal Equipment (DTE) - Usually a customer owned device that provides connectivity between company's own network and the frame relay's network.

For your exam you should know below information about WAN Technologies:

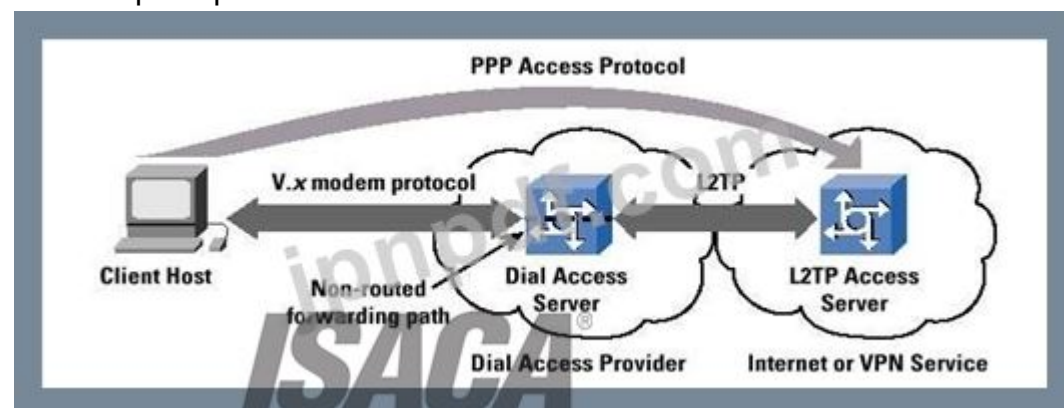
Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP uses the Internet protocol (IP) (and is designed to handle other protocol as well). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation. PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Point-to-point protocol



X.25

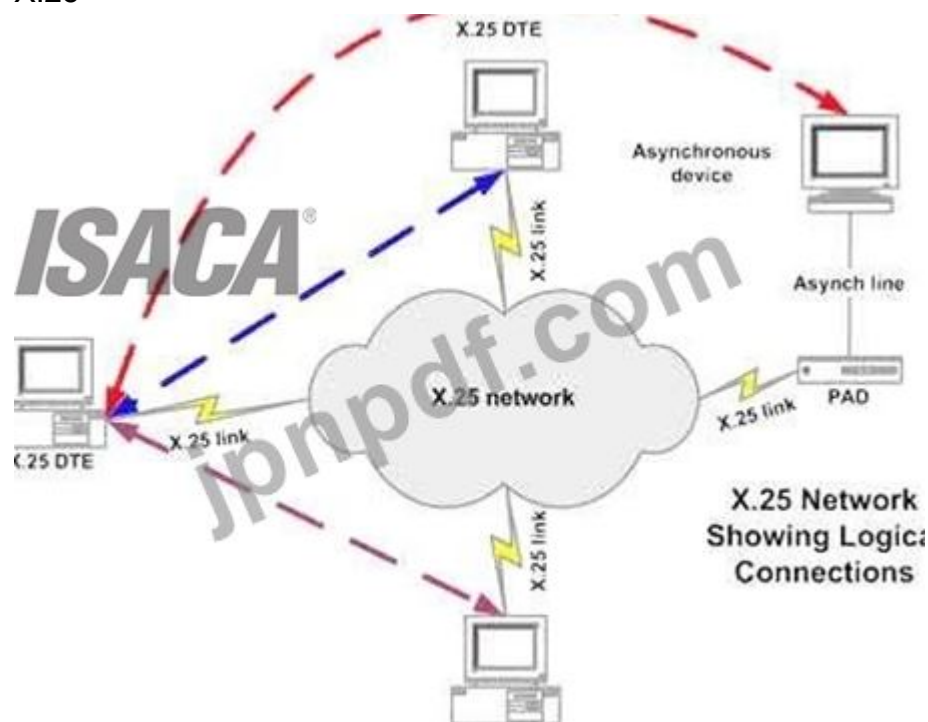
X.25は、パケット交換広域ネットワーク（WAN）通信のためのITU-T標準プロトコルスイートです。

X.25は、キャリアスイッチを使用してさまざまなネットワークへの接続を提供するパケット交換技術です。

加入者は使用する帯域幅の量に基づいて料金を請求されます。データは128バイトに分割され、高レベルデータリンク制御（HDLC）でカプセル化されます。

X.25はOSIモデルのネットワーク層とデータリンク層で動作します。

X.25



フレームリレー

パケット交換として機能します

OSIモデルのデータリンク層で動作します。

より高いレベルの帯域幅が常に利用可能であることを保証するために、より多くの料金を支払う企業は、コミットメント情報レート (CIR)を支払います。フレームリレーでは主に2種類の機器が使用されます。

1. データ端末装置 (DTE) - 通常は顧客所有のデバイスで、企業のネットワークとフレームリレーのネットワーク間の接続を提供します。
2. データ回線端末装置 (DCE) - フレームリレークラウド内で実際のデータ伝送とスイッチングを行うサービスプロバイダのデバイス。

フレームリレークラウドは、スイッチング機能とデータ通信機能を提供するDCE (データセンターエクスチェンジ)の集合体です。フレームリレーは、あらゆるサービス間の通信を可能にします。

フレームリレー



統合サービスデジタルネットワーク (ISDN)

データ、音声、その他の種類のトラフィックを、従来アナログ音声伝送にのみ使用されていた媒体上でデジタル方式で伝送することを可能にする。

従来の電話回線 (POTS) 上で動作します。同じ銅製の電話線が使用されます。

デジタルポイントツーポイント回線交換媒体を提供する。

ISDN

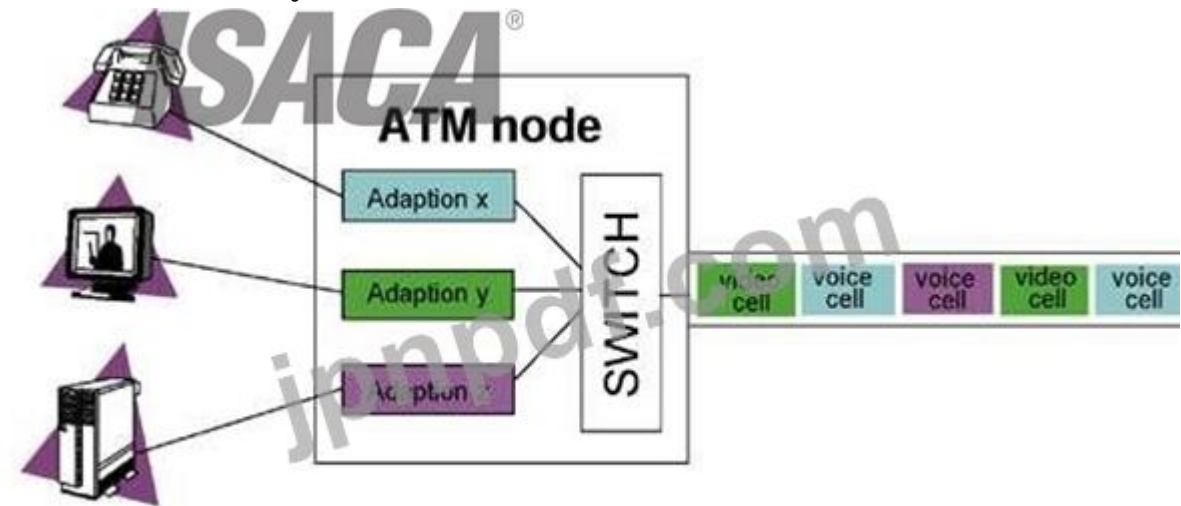


非同期転送モード (ATM)

セルスイッチング方式を採用

LAN、MAN、WANで使用する高速ネットワーク技術

フレームリレーと同様に、これは接続指向の技術であり、固定チャネルを作成して使用します。データは53バイトの固定サイズのセルに分割されます。一部の企業はFDDIバックエンドをATM非同期転送モードに置き換えています。



Services	Adaptation layer	ATM layer	Physical Layer

マルチプロトコラベルスイッチング (MPLS)

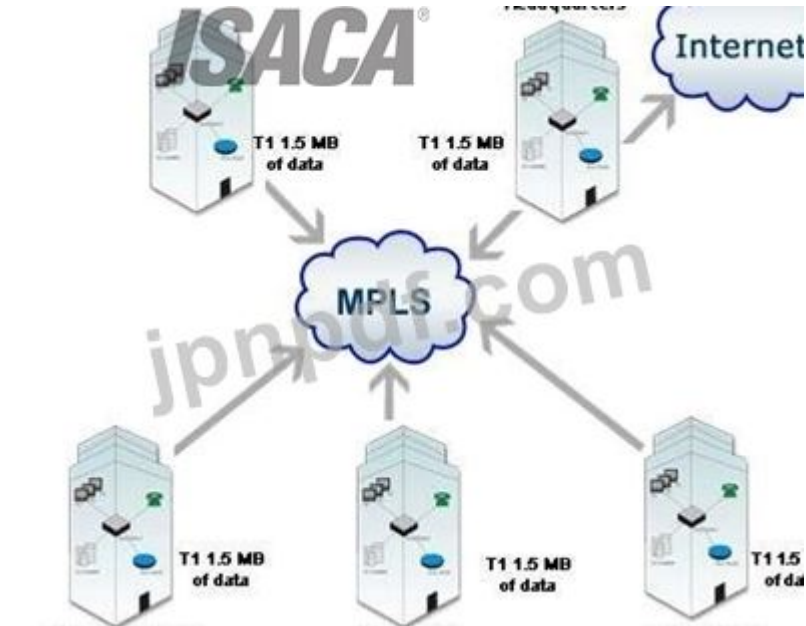
マルチプロトコラベルスイッチング (MPLS)は、ネットワークトラフィックの流れを高速化し、管理を容易にするための標準規格に準拠した技術です。MPLSでは、各パケットにラベルを付けることで、特定のパケットシーケンスに対して専用のパスを設定します。これにより、ルーターがパケットを転送する次のノードのアドレスを検索するのに必要な時間を節約できます。

MPLSは、インターネットプロトコル (IP)、非同期トランスポートモード (ATM)、およびフレームリレーネットワークプロトコルと連携して動作するため、マルチプロトコルと呼ばれています。

OSI (Open Systems Interconnection)モデルを参照すると、MPLSでは、ほとんどのパケットをレイヤ3 (ルーティング)レベルではなく、レイヤ2 (スイッチング)レベルで転送することができます。

In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

DCE - Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

DME - Not a valid frame relay technique

DLE - Not a valid frame relay technique

Reference:

CISA review manual 2014 page number 266

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **782**

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

- A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
- B. The service provider does not have incident handling procedures.
- C. Recently a corrupted database could not be recovered because of library management problems.
- D. incident logs are not being reviewed.

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

最新問題: **783**

Which of the following MOST effectively provides assurance of ongoing service delivery by a vendor?

- A. Regular status reporting provided by the vendor
- B. Short incident response time by the vendor
- C. Pre-defined service and operational level agreements
- D. Regular monitoring by service management team

Answer: C ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

最新問題: **784**

小規模なeコマース企業の経営陣は、AIの導入が自社の知的財産に与える影響を懸念している。この懸念に最も適切に対応できるのは次のうちどれか？

- A. AIの許容利用ポリシーの策定

- B. 生成型AIを使用した従業員への制裁
- C. AIウェブトラフィックログの手動レビューの実施
- D. チャットベースのAIウェブサイトとプラグインを拒否リストに追加する

Answer: A ([メッセージを残す](#))

最善のアプローチは、従業員が機密情報や知的財産を保護しながらAIツールをどのように使用できるかを明確に定義した、AIの適切な利用に関するポリシーを策定することです。これにより、ガバナンスを確保しつつ、安全な導入が可能になります。

選択肢B：予防的ではなく、事後対応的かつ懲罰的な統治。

選択肢C：監視は役立つが、それだけでは不十分である。

選択肢D：過度に制限的であり、有益なAIの利用を阻害する可能性がある。

選択肢A：正解 ポリシーは、事業目標とリスク管理に沿った体系的なガイダンスを提供する。

最新問題: 785

ある銀行が、システムを他国に拠点を置くクラウドプロバイダーにアウトソーシングすることを希望しています。以下のうち、最も適切な情報システム監査の推奨事項はどれでしょうか？

- A. 銀行の本国で代替のプロバイダーを探してください。
- B. プロバイダーの内部統制システムが銀行の要件を満たしていることを確認する。
- C. 予定通りに進めてください。プロバイダーはクライアントの国のすべての法律を遵守する必要があります。
- D. プロバイダーが災害復旧能力を備えていることを確認してください。

Answer: ([解答を表示する](#))

実施後レビュー（PIR）とは、プロジェクトの目標が達成されたかどうかを評価し、その達成度を判断し、将来のための教訓を学び、組織がプロジェクトの実施から最大限の利益を得られるようにするためのプロセスです¹。PIRは、プロジェクトの成功と価値を評価するだけでなく、改善すべき領域や将来のプロジェクトにおけるベストプラクティスを特定するための重要なツールです。

PIRの重要な要素の1つは、プロジェクトの開始時に定義された期待される成果とメリットに対して、プロジェクトのメリットを測定することです。測定可能なメリットとは、収益の増加、コストの削減、品質の向上、顧客満足度の向上、規制への準拠など、プロジェクトが組織またはその利害関係者にもたらす定量化可能で検証可能な結果または成果のことです²。

測定可能なメリットは、組織の戦略、ビジョン、目標と整合している必要があります、SMART（具体的測定可能、達成可能、関連性があり、期限が明確）であるべきです。

測定可能な利益が定義されていなかったという発見は、4つの発見の中で最も重要なものであり、それは次のことを示唆している。

- * このプロジェクトには、明確かつ合意された目的、範囲、目標、成果物が存在しなかった。
 - * このプロジェクトには、開始および実施のための有効かつ現実的なビジネスケースや正当性は存在しなかった。
 - * このプロジェクトには、進捗状況、成果、影響を追跡するための堅牢かつ効果的なモニタリングおよび評価メカニズムがなかった。
 - * このプロジェクトには、組織やその利害関係者に対して、その価値提案と投資収益率を信頼性高く透明性をもって示す方法がなかった。
 - * このプロジェクトには、成果や課題から学び、プロセスや慣行を改善するための有意義で実行可能な方法がありませんでした。
- したがって、IS監査人は、プロジェクトの実施前に測定可能なメリットを定義し、プロジェクトの実施中および完了後に定期的にレビューおよび報告することを推奨する必要があります。

その他の可能性のある所見は以下のとおりです。

* 教訓セッションは一度も実施されなかった: これは重要な発見だが、

* 測定可能なメリットの欠如。教訓セッションとは、プロジェクトから得られた知識、経験、フィードバック（肯定的および否定的）を収集し、文書化するプロセスです。教訓セッションは、プロジェクト管理プロセスの強みと弱み、および将来のプロジェクトのためのベストプラクティスと教訓を特定するのに役立ちます。教訓セッションは、各プロジェクトフェーズまたはマイルストーンの終了時、およびプロジェクトの終了時に実施する必要があります。ただし、正式な教訓セッションがなくても、プロジェクトチームメンバーやステークホルダーの間で、非公式または暗黙のうちに何らかの学習が行われる可能性があります。

* The projects 10% budget overrun was not reported to senior management: This is a significant finding, but not as significant as the lack of measurable benefits. A budget overrun is a situation where the actual cost of a project exceeds its planned or estimated cost. A budget overrun may indicate poor planning, estimation, or control of the project resources, or unexpected changes or risks that occurred during the project implementation. A budget overrun should be reported to senior management as soon as possible, along with the reasons for it and the corrective actions taken or proposed. However, a budget overrun may not necessarily affect the quality or value of the project deliverables or outcomes if they are still within acceptable standards or expectations.

* Monthly dashboards did not always contain deliverables: This is a significant finding, but not as significant as the lack of measurable benefits. A dashboard is a visual tool that displays key performance indicators (KPIs) or metrics related to a project's progress, status, or results. A dashboard helps to monitor and communicate the performance of a project to various stakeholders in a concise and clear manner. A dashboard should include deliverables as one of its components, along with other elements such as schedule, budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.

References: 1: The role & importance of the Post Implementation Review 2: What is Post-Implementation Review in Project Management?

最新問題: 786

On a public-key cryptosystem when there is no previous knowledge between parties, which of the following will BEST help to prevent one person from using a fictitious key to impersonate someone else?

- A. Encrypt the message containing the sender's public key, using a private-key cryptosystem.
- B. Send a certificate that can be verified by a certification authority with the public key.
- C. Encrypt the message containing the sender's public key; using the recipient's public key.
- D. Send the public key to the recipient prior to establishing the connection.

Answer: ([解答を表示する](#))

25 of 150

ISACA®

In data warehouse (DW) management, what is the **BEST** way to prevent data quality issues caused by changes from a source system?

- ☐ Restrict access to changes in the extract/transfer/load (ETL) process between the two systems.
- ☐ Configure data quality alerts to check variances between the data warehouse and the source system.
- ☐ Require approval for changes in the extract/transfer/load (ETL) process between the two systems.
- ☒ Include the data warehouse in the impact analysis for any changes in the source system.

最新問題: 787

An organization has virtualized its server environment without making any other changes to the network or security infrastructure. Which of the following is the MOST significant risk?

- A. Vulnerability in the virtualization platform affecting multiple hosts
- B. Data center environmental controls not aligning with new configuration
- C. Inability of the network intrusion detection system (IDS) to monitor virtual server-to-server communications.
- D. System documentation not being updated to reflect changes in the environment

Answer: A ([メッセージを残す](#))

最新問題: 788

事業継続計画 (BCP)の監査中に、情報システム監査担当者は、すべての部署が同じ建物内に配置されているにもかかわらず、各部署がそれぞれ別のBCPを作成していることを発見しました。情報システム監査担当者は、これらのBCPを統合させるよう勧告しました。以下のどの領域を最初に統合させるべきでしょうか？

- A. 避難計画
- B. 復旧の優先事項
- C. バックアップストレージ
- D. コールツリー

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

災害発生時の人的資源の保護は、最優先事項として取り組むべき課題です。事業継続計画 (BCP)が部門ごとに異なると、避難計画に矛盾が生じ、職員や顧客の安全が脅かされる可能性があります。選択肢B、C、Dは各部門固有のものであり、個別に検討することも可能ですが、人的安全の問題を分析した後でなければ、潜在的な矛盾やコスト削減の可能性について検討すべきです。

最新問題: 789

ある組織のセキュリティチームが、複数の脆弱性のあるアプリケーションを含む模擬的な本番環境を作成しました。このような環境を作成する主な目的は何でしょうか？

- A. サイバー攻撃のデジタル証拠を収集する
- B. 攻撃者の行動を研究するために攻撃者を誘い込む
- C. セキュリティ管理者への研修を提供する
- D. 侵入検知システム (IDS)のテスト

Answer: B ([メッセージを残す](#))

複数の脆弱なアプリケーションを含む模擬的な本番環境を作成する主な目的は、攻撃者を引き付けてその行動を研究することです。これはハニーポットティングと呼ばれる手法で、攻撃者を実際のシステムを模倣した偽のシステムまたはネットワークに誘い込む欺瞞型セキュリティの一種ですが、そのシステムは隔離され監視されています¹。ハニーポットティングは、セキュリティチームが攻撃者の手法、ツール、動機、およびターゲットについて学び、組織のセキュリティ体制を改善するために使用できる貴重な情報を収集するのに役立ちます¹。ハニーポットティングは、攻撃者の注意を実際の資産からそらし、時間とリソースを浪費するのにも役立ちます²。

その他のオプションは、複数の脆弱なアプリケーションを含む模擬的な本番環境を作成する主な目的ではありません。サイバー攻撃のデジタル証拠を収集するには、セキュリティチームは、侵害されたシステムまたはネットワークからデータを保存および

分析できるフォレンジックツールと技術を使用する必要があります3。セキュリティマネージャーにトレーニングを提供するには、セキュリティチームは、サイバーインシデントへの対応におけるスキルと知識をテストおよび向上できるシミュレーションツールとシナリオを使用する必要があります4。侵入検知システム (IDS) をテストするには、セキュリティチームは、悪意のある活動を検出および防止するIDSの有効性とパフォーマンスを評価できる侵入テストツールと方法を使用する必要があります5。

参考文献：

ハニーポットとは？ | Imperva

ハニーポット：侵入者を特定するための甘い解決策 | CSO Online

デジタルフォレンジック - 概要 | ScienceDirect Topics

サイバーセキュリティ訓練と演習 - 国土安全保障省

ペネトレーションテストとは？ | 種類と段階 | Imperva

最新問題: 790

ビジネス継続性監査を実施する際に、情報システム監査担当者が検証すべき最も重要な項目は次のうちどれでしょうか？

- A. データバックアップは定期的の実施されます
- B. 回収場所は契約済みで、必要に応じて利用可能です。
- C. 人的安全対策が実施されています
- D. 保険適用範囲は十分であり、保険料は滞納されていない。

Answer: C ([メッセージを残す](#))

事業継続計画において最も重要な要素は、人命の保護である。これは計画の他のあらゆる側面よりも優先される。

最新問題: 791

Passwords should be:

- A. assigned by the security administrator for first time logon.
- B. changed every 30 days at the discretion of the user.
- C. reused often to ensure the user does not forget the password.
- D. displayed on the screen so that the user can ensure that it has been entered properly.

Answer: A ([メッセージを残す](#))

Explanation/Reference:

Explanation:

Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

最新問題: 792

以下のうち、自己評価によるコントロール (CSA) の主な利点はどれですか？

- A. 経営目標を支える内部統制に対する経営陣の責任が強化される。
- B. 評価結果が外部監査業務のインプットとなる場合、監査費用は削減されます。
- C. 内部業務スタッフがテスト管理に携わることで、不正検出能力が向上しました。
- D. 内部監査人は、評価結果を利用してコンサルティング的なアプローチに移行することができます。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

内部統制の自己評価の目的は、企業経営陣が内部統制の重要性と、コーポレートガバナンスにおける自らの責任について、より深く認識することにある。

Reducing audit expenses is not a key benefit of control self-assessment (CSA). improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

最新問題: 793

An intruder accesses an application server and makes changes to the system log. Which of the following would enable the identification of the changes?

- A. Storing the backup of the system log offsite
- B. Mirroring the system log on another server
- C. Simultaneously duplicating the system log on a write-once disk
- D. Write-protecting the directory containing the system log

Answer: D ([メッセージを残す](#))

最新問題: 794

ITプロジェクトにおけるプライバシーに関する懸念の範囲を評価する際に、最も重要な考慮事項は次のうちどれですか？

- A. データ所有権
- B. 適用される法律および規制
- C. ビジネス要件とデータフロー
- D. エンドユーザーのアクセス権限

Answer: B ([メッセージを残す](#))

ITプロジェクトにおけるプライバシーに関する懸念の範囲を評価する際に考慮すべき最も重要な要素は、適用される法律および規制です。これらの法律および規制は、プロジェクトが遵守しなければならないデータプライバシーおよび保護に関する法的要件を定めています。これらは管轄区域や処理されるデータの種類によって大きく異なる場合があります、不遵守は重大な罰則につながる可能性があります¹²³。データの所有権、ビジネス要件とデータフロー、エンドユーザーのアクセス権も重要な考慮事項ですが、これらは通常、これらの法的要件によって規定されます。

参考文献 :ISACAの情報システム監査人学習教材1

最新問題: 795

組織のシステムが分散型サービス拒否 (DDoS) 攻撃に参加するのを防ぐのに役立つのは、次のうちどれですか？

- A. 受信トラフィックのフィルタリング
- B. アクセス制御リスト (ACL) を使用して、受信接続試行を制限する
- C. 送信トラフィックのフィルタリング
- D. 分散システムの再集中化

Answer: (解答を表示する)

セクション：情報資産の保護

Explanation:

送信トラフィックのフィルタリングは、組織のシステムが分散型サービス拒否（DDoS）攻撃に
関与するのを防ぐのに役立ちます。

最新問題: 796

ネットワーク環境は、プログラム間の通信を複雑化させ、アプリケーションシステムの導入と保守をより困難にすることが多い。
正誤を答えよ。

A. 真

B. 偽

Answer: A ([メッセージを残す](#))

説明／参考資料：

ネットワーク環境は、プログラム間の通信を複雑化させることが多く、アプリケーションシステムの導入と保守をより困難にする。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 797

IS監査人が職務分掌が実施されていることを検証する最良の方法は、以下の手順を実行することです。

A. 人事ファイルの確認。

B. 文書化された職務記述書の分析。

C. 組織図の見直し。

D. 職務内容の説明。

Answer: D ([メッセージを残す](#))

職務遂行状況の観察は、職務分掌（SoD）が効果的に実施されていることを示す直接的な証拠となる。これは、従業員が業務を遂行する様子を観察し、特定の個人が過剰な権限を持っていないことを確認するものである。

職務内容の解説（正解D）

実際の業務において、職務が適切に分担されていることを確認する。

セキュリティポリシーと制御が適切に実施されているかどうかを確認するのに役立ちます。

例：監査人が、同一人物が財務取引を作成および承認することはできないと指摘する。

人事ファイルのレビュー（不正解 A）

人事ファイルには職務内容の詳細が記載されているが、職務がどのように遂行されたかは確認できない。

文書化された職務記述書の分析（不正解 B）

職務内容の説明が古くなっていたり、不正確だったりする可能性があります。

組織図の見直し（誤り - C）

報告関係は示されているが、職務分掌（SoD）の実装は確認されていない。

参考文献：

最新問題: 798

Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor s BEST recommendation for a compensating control?

- A. Review payment transaction history.
- B. Reconcile payment transactions with invoices.
- C. Require written authorization for all payment transactions.
- D. Restrict payment authorization to senior staff members

Answer: B ([メッセージを残す](#))

最新問題: 799

組織のネットワークへの侵入が検出された場合、最初に行うべきことは次のうちどれですか？

- A. 上級管理職に報告する。
- B. 侵害されたノードを特定する。
- C. 侵害されたネットワークノードをすべてブロックします。
- D. 警察に連絡してください。

Answer: D ([メッセージを残す](#))

最新問題: 800

Which of the following MOST effectively mitigates the risk of disclosure of sensitive data stored on company-owned smartphones?

- A. Physical device tagging
- B. Secure containers
- C. Mobile device management (MDM)
- D. Data leakage prevention (DLP) tools

Answer: D ([メッセージを残す](#))

最新問題: 801

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST

- A. issue an intermediate report to management.
- B. evaluate the impact on current disaster recovery capability.
- C. perform a business impact analysis (BIA).
- D. conduct additional compliance testing.

Answer: D ([メッセージを残す](#))

最新問題: 802

Which of the following is MOST important for an IS auditor to review when assessing the integrity of encryption controls for data at rest?

- A. Length of encryption keys
- B. Encryption of test data
- C. Protection of encryption keys
- D. Frequency of encryption key changes

Answer: [\(解答を表示する\)](#)

最新問題: **803**

During a vulnerability assessment, an IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer orders via credit card. The IS auditor should FIRST:

- A. notify management.
- B. redesign the customer order process.
- C. document the finding in the report.
- D. suspend credit card processing.

Answer: C ([メッセージを残す](#))

Section: The process of Auditing Information System

最新問題: **804**

Which of the following would present the GREATEST concern during a review of internal audit quality assurance (QA) and continuous improvement processes?

- A. Improvement opportunities are not centrally tracked.
- B. The audit function is not subject to independent periodic external review.
- C. Substantive testing is not performed during the assessment phase of some audits.
- D. Quarterly reports are not distributed to the audit committee.

Answer: B ([メッセージを残す](#))

The best answer is B.

A quality assurance and improvement program is meant to evaluate whether the audit function is performing effectively and independently. ISACA's candidate guide explicitly includes evaluating audit processes as part of QA and improvement programs, and ISACA peer-review guidance states that a peer review process assessing internal audit is essential to ensure it is appropriately carrying out its role. The absence of independent periodic external review is therefore the most serious concern because it weakens objective assessment of audit quality itself.

Option A is a weakness, but tracking improvement opportunities centrally is secondary to having independent validation that the function meets expected quality standards. Option C is not the best answer because substantive testing during an assessment phase may vary by engagement design. Option D matters for governance communication, but it is still less central to QA than the lack of external independent review.

References (Official ISACA):

- * ISACA, Certification Exam Candidate Guide.
- * ISACA Journal, A Standardized Approach for Peer Review of Internal Audit.

最新問題: **805**

事業継続計画 (BCP) を策定する際、最初に行うべき手順は次のうちどれですか？

- A. 事業主と復旧時間と復旧プロセスの目標について話し合う
- B. リスク評価を実施する
- C. ITコンポーネントの復旧に適した制御と対策を選択する。
- D. 事業継続戦略を策定する

Answer: ([解答を表示する](#))

最新問題: 806

経営陣は、従業員が意図的または意図せず機密情報を添付ファイルとして組織外にメールで送信してしまうことを懸念しています。関連するメール管理策を実施する前に、最も重要なタスクは何でしょうか？

- A. 全従業員に秘密保持契約 (NDA) への署名を義務付ける。
- B. エンドユーザーコンピューティング (EUC) の許容使用ポリシーを作成する。
- C. 情報分類体系を開発する。
- D. 従業員に対し、メール監視の可能性について通知する。

Answer: C ([メッセージを残す](#))

説明

従業員が機密情報を組織外に電子メールで送信するのを防ぐための関連する電子メール制御を導入する前に、最も重要な作業は、情報分類スキームを策定することです。

情報分類スキームとは、公開情報、内部情報、機密情報、秘密情報など、さまざまな種類の情報のカテゴリと機密レベルを定義するフレームワークです。情報分類スキームは、電子メールの添付ファイル内の機密情報を識別、ラベル付け、処理、保護するための基準とガイドラインを提供することで、電子メール制御の実装に役立ちます。他のオプションは、問題の根本原因に対処したり、同じメリットを提供したりしないため、情報分類スキームの開発ほど重要ではありません。すべての従業員に秘密保持契約 (NDA) への署名を求めることは、従業員が機密情報を開示することを抑止または罰するのに役立つ法的制御ですが、従業員が組織外に電子メールで送信することを防ぐことはできません。エンドユーザーコンピューティング (EUC) の許容使用ポリシーを作成することは、電子メールなどのITリソースの使用に関するルールと期待を定義して伝えるのに役立つガバナンス制御ですが、従業員が組織外に機密情報を電子メールで送信することを防ぐことはできません。従業員にメール監視の可能性について通知することは、組織外に機密情報をメールで送信した場合の潜在的な影響について従業員に情報を提供し、警告するのに役立つ透明性管理策ですが、従業員がそうすること自体を阻止するものではありません。参照 :CISAレビューマニュアル (デジタル版)、第5章、セクション5.3.2

最新問題: 807

An IS auditor notes that IT and the business have different opinions on the availability of their application servers. Which of the following should the IS auditor review FIRST in order to understand the problem?

- A. The exact definition of the service levels and their measurement
- B. The alerting and measurement process on the application servers
- C. The actual availability of the servers as part of a substantive test
- D. The regular performance-reporting documentation

Answer: ([解答を表示する](#))

Explanation

The exact definition of the service levels and their measurement is the first thing that the IS auditor should review in order to understand the problem of different opinions on the availability of their application servers.

Service levels are the agreed-upon standards or targets for delivering IT services, such as availability, reliability, performance, and security. Service level measurement is the process of collecting, analyzing, and reporting data related to the achievement of service levels. By reviewing the exact definition of the service levels and their measurement, the IS auditor can identify any gaps, inconsistencies, or ambiguities that may cause confusion or disagreement among IT and the business. The other options are not as important as reviewing the exact definition of the service levels and their measurement, as they do not address the root cause of the problem. References: CISA Review Manual, 27th Edition, page 372

最新問題: 808

データベースの内部監査の結果、経営陣はパスワード管理の強化に取り組むことを決定しました。経営陣が監査結果に対応したことを示す最も適切な証拠はどれですか？

- A. 経営陣への是正措置完了に関するインタビュー
- B. 最近のパスワード設定更新に関するチケットの変更
- C. エンドユーザーから提供された、更新されたパスワード設定を示すスクリーンショット
- D. データベース管理者 (DBA) によるパスワード設定の更新状況の確認

Answer: B ([メッセージを残す](#))

最新問題: 809

An IS auditor is reviewing database fields updated in real-time and displayed through other applications in multiple organizational functions. When validating business approval for these various use cases, which of the following sources of information would be the BEST starting point?

- A. Network map from the network administrator
- B. Historical database change log records
- C. List of integrations from the database administrator (DBA)
- D. Business process flow from management

Answer: ([解答を表示する](#)**)**

Understanding the business process flow is crucial as it provides insights into how different applications and organizational functions use and update the database fields in real-time. This perspective helps the auditor validate that appropriate business approvals are in place for these use cases.

References

* ISACA CISA Review Manual 27th Edition, Page 128-129 (Business Process Flow)

最新問題: 810

Which of the following would be of GREATEST concern to an IS auditor receiving an organization's security incident handling procedures?

- A. Annual tabletop exercises are performed instead of functional incident response exercises.
- B. Roles for computer emergency response team (CERT) members have not been formally documented.
- C. Guidelines for prioritizing incidents have not been identified.
- D. Workstation antivirus software alerts are not regularly reviewed.

Answer: ([解答を表示する](#)**)**

Section: Information System Operations, Maintenance and Support

最新問題: 811

新しいアプリケーションシステムの継続性計画を開始するのに最適な時期はいつですか？

- A. ユーザーテストが成功した後
- B. 設計段階で
- C. システム保守グループへの引き継ぎ直前
- D. 実施直後

Answer: (解答を表示する)

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 812

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data is accurately entered into the system?

- A. Reasonableness checks for each cost type
- B. Validity checks, preventing entry of character data
- C. Display back of project detail after entry
- D. Reconciliation of total amounts by project

Answer: A (メッセージを残す)

最新問題: 813

An IS auditor finds ad hoc vulnerability scanning is in place with no clear alignment to the organization's wider security threat and vulnerability management program.

Which of the following would BEST enable the organization to work toward improvement in this area?

- A. Implementing security logging to enhance threat and vulnerability management
- B. Maintaining a catalog of vulnerabilities that may impact mission-critical systems
- C. Using a capability maturity model to identify a path to an optimized program
- D. Outsourcing the threat and vulnerability management function to a third party

Answer: C (メッセージを残す)

The best way to enable the organization to work toward improvement in its security threat and vulnerability management program is to use a capability maturity model to identify a path to an optimized program. A capability maturity model is a framework that helps organizations assess their current level of performance and maturity in a specific domain, and provides guidance and best practices to achieve higher levels of excellence¹². A capability maturity model for vulnerability management can help the organization to evaluate its current practices, identify gaps and weaknesses, and implement improvement actions based on the defined criteria and objectives³⁴.

References

1: What is a Capability Maturity Model? 2: Capability Maturity Model - Wikipedia 3: Vulnerability Management Maturity Model - SANS Institute 4: 5 Stages Of Vulnerability Management Maturity Model - SecPod Blog

最新問題: 814

オンライン注文入力システムへの更新処理が行われると、その更新内容はトランザクションテープに記録される。そして、紙の取引記録。一日の終わりに、注文入力ファイルはテープにバックアップされます。バックアップ手順中にドライブが故障し、注文入力ファイルが失われました。次のうちどれがこれらのファイルを復元するために必要ですか？

- A. 前日のバックアップファイルと現在のトランザクションテープ
- B. 前日の取引ファイルと現在の取引テープ
- C. 現在の取引テープと現在の紙媒体の取引ログ
- D. 現在の紙媒体の取引記録と前日の取引ファイル

Answer: A ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

前日のバックアップファイルは、システム内のアクティビティの最新の履歴バックアップとなります。当日のトランザクションファイルには、その日のすべてのアクティビティが含まれます。したがって、これら2つの組み合わせはこれらのファイルにより、中断時点までの完全な復旧が可能になります。

最新問題: 815

IS監査担当者は、サービスプロバイダーがセキュリティ侵害について顧客に通知していなかったことを発見した場合、まず最初に何をすべきでしょうか？

- A. 発見内容を法執行機関に通知する。
- B. 第三者に顧客への通知を要求する。
- C. 重大な発見事項を含む監査報告書。
- D. 監査管理者に調査結果を通知する。

Answer: D ([メッセージを残す](#))

IS監査担当者は、監査範囲と目的に影響を与える可能性のある重大な問題であるため、まず監査管理部門に発見事項を通知する必要があります。IS監査担当者は、監査管理部門と事前に協議することなく、法執行機関に通知したり、第三者に顧客への通知を要求したりしてはなりません。重大な発見事項を含む監査報告書は、監査が完了し、発見事項が検証された後に発行する必要があります。参考文献 :ISACA、CISAレビューマニュアル、第27版、2018年、247ページ

最新問題: 816

Which of the following will MOST likely compromise the control provided by a digital signature created using RSA encryption?

- A. Deciphering the receiver's public key
- B. Altering the plaintext message
- C. Reversing the hash function using the digest
- D. Obtaining the sender's private key

Answer: ([解答を表示する](#))

最新問題: 817

Which of the following is the BEST control to mitigate the malware risk associated with an instant messaging (IM) system1?

- A. Blocking attachments in IM
- B. Blocking external IM traffic
- C. Encrypting IM traffic
- D. Allowing only corporate IM solutions

Answer: D ([メッセージを残す](#))

最新問題: 818

To effectively classify data, which of the following MUST be determined?

- A. Data ownership
- B. Data controls
- C. Data users
- D. Data volume

Answer: A ([メッセージを残す](#))

最新問題: 819

アプリケーションの設計に深く関わったIS監査担当者が、そのアプリケーションのレビューを依頼された。監査担当者は以下のことを行うべきである。

- A. 監査範囲の変更
- B. 監査管理への早期関与
- C. 利益相反を避けるため、依頼を拒否する
- D. アプリケーションの知識を活用して監査を実施する

Answer: ([解答を表示する](#)**)**

最新問題: 820

What is the primary objective of a control self-assessment (CSA) program?

- A. Enhancement of the audit responsibility
- B. Elimination of the audit responsibility
- C. Replacement of the audit responsibility
- D. Integrity of the audit responsibility

Answer: ([解答を表示する](#)**)**

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

最新問題: 821

組織の災害復旧計画 (DRP)における復旧時間目標 (RTO)の達成を確実にするアプローチは、次のうちどれでしょうか？

- A. サイバーレジリエンステストの実施
- B. 完全中断テストの実施

C. 卓上テストの実施

D. 並列テストの実施

Answer: [\(解答を表示する\)](#)

説明

完全中断テストは、組織の災害復旧計画（DRP）における復旧時間目標（RTO）が達成されていることを確認するための、最も現実的かつ信頼性の高い方法です。RTOとは、災害発生後に企業がオフライン状態を許容できる最大時間です。完全中断テストでは、プライマリサイトをシャットダウンし、バックアップサイトに切り替えることで、実際の災害シナリオをシミュレートします。このテストにより、事業継続に不可欠なシステム、アプリケーション、および機能を復旧するのにかかる実際の時間を測定できます。また、完全中断テストは、復旧プロセスに影響を与える可能性のあるDRPの問題点や欠陥を明らかにするのにも役立ちます。他のオプションは、RTO が満たされていることを確認するための完全な中断テストほど効果的ではありません。サイバーレジリエンス テストは、サイバー攻撃に耐え、そこから復旧する能力に焦点を当てた DR テストの一種です。他の種類の災害を必ずしもカバーしたり、DRP 全体をテストしたりするわけではありません。テーブルトップ テストは、主要な関係者とスタッフとともに DRP をウォークスルーする影響の少ない DR テストです。バックアップ システムの実際の切り替えやテストは含まれません。パラレル テストは、通常の運用を中断することなく、プライマリ システムと並行してバックアップ システムを実行する DR テストの一種です。バックアップ サイトで切り替えや運用再開にかかる時間は測定されません。

参考文献：

災害復旧テストのベストプラクティス

災害復旧テスト

災害復旧テスト：知っておくべきことすべて

最新問題: 822

デジタル署名の特徴は、

A. 受信機の制御下にある

B. メッセージに固有のものです

C. データが変更されたときに検証されます

D. 再現可能なハッシュアルゴリズムを備えている

Answer: B ([メッセージを残す](#))

デジタル署名は、デジタル証明書によって裏付けられた電子署名の一種です。デジタル証明書とは、署名者の公開鍵を含む文書であり、認証局（CA）と呼ばれる信頼できる第三者機関によって発行されます。デジタル署名は、署名者の身元と署名された文書の完全性を証明するものです。

デジタル署名の特徴の一つは、メッセージごとに固有であることです。つまり、デジタル署名は、ある文書から別の文書にコピーすると、無効と判定されます。デジタル署名は、ハッシュアルゴリズムと呼ばれる数学的関数を文書に適用することで作成されます。ハッシュアルゴリズムは、入力データからハッシュまたはダイジェストと呼ばれる固定長の出力を生成します。ハッシュは入力データごとに固有であり、入力データに変更があると、生成されるハッシュも異なります。

署名者は、自身の秘密鍵（署名者のみが知っている秘密の鍵）でハッシュを暗号化してデジタル署名を作成します。暗号化されたハッシュは、デジタル署名として文書に添付されます。文書の受信者は、署名者の公開鍵（公開されており、秘密鍵と一致する鍵）でハッシュを復号化することで、デジタル署名を検証できます。受信者は、同じハッシュアルゴリズムを文書に適用して、別のハッシュを生成します。受信者は、2つのハッシュを比較します。ハッシュが一致すれば、文書が改ざんされておらず、署名者が正当な人物であると判断できます。

したがって、デジタル署名はメッセージのハッシュ値から生成されるため、メッセージ固有のものとなります。

参考文献：

* 7：無料オンライン署名ジェネレーター（入力または描画） | Signaturely

* 8：デジタル署名と証明書とは何ですか？ | Acrobat Sign - Adobe

* 9: eSign PDF に電子署名を無料でオンラインで適用 - Smallpdf

最新問題: 823

The business owner's approval of software changes being moved into production is PRIMARILY necessary to:

- A. prevent unauthorized access to data.
- B. inform management of deployments of new functionality.
- C. confirm there is a process to control system changes.
- D. ensure that an application functionality requirement is satisfied.

Answer: B ([メッセージを残す](#))

最新問題: 824

When planning an end-user computing (EUC) audit, it is MOST important for the IS auditor to:

- A. determine EUC materiality and complexity thresholds.
- B. obtain an inventory of EUC applications.
- C. evaluate the organization's EUC policy.
- D. evaluate EUC threats and vulnerabilities.

Answer: (解答を表示する)

最新問題: 825

IS監査の結果、ITアプリケーションのパフォーマンスが低下しており、データ不整合やデータ整合性の問題が発生していることが判明しました。最も可能性の高い原因は何でしょうか？

- A. データベースクラスタリング
- B. データキャッシュ
- C. データベーステーブルのインデックス再構築
- D. ロードバランシング

Answer: B ([メッセージを残す](#))

説明

データキャッシュは、ITアプリケーションのパフォーマンス低下、データの一貫性の欠如、データの整合性の問題を引き起こす可能性が最も高い原因です。これは、頻繁にアクセスされるデータを一時的なメモリ領域（キャッシュ）に保存することで、元のソースからデータを取得する際の遅延と帯域幅の消費を削減するためです。しかし、データキャッシュは、古いデータ（キャッシュが元のソースへの変更で更新されない場合）、キャッシュの一貫性（複数のキャッシュが同じデータのコピーを保存し、同期が必要な場合）、キャッシュの破損（キャッシュが破損または改ざんされた場合）などの問題を引き起こす可能性もあります。

データベースクラスタリングは、複数のサーバーまたはノードにデータを分散させることでデータベース操作の可用性、拡張性、負荷分散を向上させるため、パフォーマンスの低下、データの不整合、整合性の問題を引き起こす可能性は低い。また、データベースクラスタリングは、レプリケーションと同期メカニズムを使用してすべてのノードが同じデータビューを持つことを保証することで、データの一貫性と整合性を向上させることもできる。

データベーステーブルのインデックス再構築は、パフォーマンスの低下、データの不整合、データの整合性の問題を引き起こす可能性は低い。なぜなら、インデックス再構築は、テーブルまたはビュー上のインデックスを再構築または再編成することで、クエリのパフォーマンスを向上させ、インデックスページの断片化を軽減するからである。また、インデックス再構築は、インデックスがテーブルまたはビュー内のデータの現在の状態を反映するようにすることで、データの整合性と整合性を向上させることもできる。

負荷分散は、複数のサーバーやリソースにワークロードを分散させることで、アプリケーションのリソース利用率、スループット、応答時間を最適化するため、パフォーマンスの低下、データの不整合、整合性の問題を引き起こす可能性は低いと言えます。負荷分散は、可用性、容量、パフォーマンスに基づいて、最も適切なサーバーやリソースにリクエストをルーティングするアルゴリズムとプロトコルを使用することで、データの一貫性と整合性を向上させることもできます。

参考文献：

データキャッシュ

データベースクラスタリング

SQL Server でデータベース テーブルのインデックスを再構築する
[ロード]

最新問題: 826

情報セキュリティポリシーの策定において、ビジネス目標との整合性を最も確実に確保できるのは次のうちどれでしょうか？

- A. 業界のベストプラクティスの導入
- B. 政策と手続きの連携
- C. バランススコアカードの使用
- D. 関係者からの意見

Answer: ([解答を表示する](#))

セクション：情報システムの取得、開発、導入

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 827

A data breach has occurred due to malware. Which of the following should be the FIRST course of action?

- A. Notify the cyber insurance company.
- B. Shut down the affected systems.
- C. Quarantine the impacted systems.
- D. Notify customers of the breach.

Answer: ([解答を表示する](#))

Explanation

The first course of action when a data breach has occurred due to malware is to quarantine the impacted systems. This means isolating the infected systems from the rest of the network and preventing any further communication or data transfer with them. This can help contain the spread of the malware, limit the damage and exposure of sensitive data, and facilitate the investigation and remediation of the incident. Quarantining the impacted systems can also help preserve the evidence and logs that may be needed for forensic analysis or legal action.

References:

[1] provides a guide on how to respond to a data breach caused by malware and recommends quarantining the impacted systems as the first step.

[2] explains what is malware and how it can cause data breaches, and suggests quarantining the infected devices as a best practice.

[3] describes the steps involved in quarantining a system infected by malware and the benefits of doing so.

最新問題: 828

次のうち、デジタル形式のデータをアナログ形式に変換し、再びデジタル形式に戻す通信機器はどれですか？

- A. マルチプレクサ
- B. モデム
- C. プロトコルコンバータ
- D. 濃縮器

Answer: B ([メッセージを残す](#))

モデムとは、デジタルデータをアナログデータに変換し、再びデジタルデータに戻す装置である。

最新問題: 829

An incorrect version of source code was amended by a development team, This MOST likely indicates a weakness in:

- A. change management.
- B. quality assurance (QA)
- C. project management.
- D. Incident management.

Answer: ([解答を表示する](#)**)**

最新問題: 830

How would an IS auditor BEST determine the effectiveness of a security awareness program?

- A. Review the results of social engineering tests.
- B. Evaluate management survey results.
- C. Interview employees to assess their security awareness.
- D. Review security awareness training quiz results.

Answer: ([解答を表示する](#)**)**

Comprehensive and Detailed Step-by-Step Explanation:

Social engineering tests are the most effective way to assess real-world security awareness by measuring employees' ability to recognize and resist security threats.

Review the Results of Social Engineering Tests (Correct Answer - A)

Simulated phishing attacks and pretexting exercises measure actual employee behavior.

Provides actionable insights into weaknesses in security awareness.

Example: If employees frequently click on phishing emails, the awareness program is ineffective.

Evaluate Management Survey Results (Incorrect - B)

Management perception is subjective and does not reflect actual employee behavior.

Interview Employees (Incorrect - C)

Employees may provide inaccurate or rehearsed responses.

Review Security Training Quiz Results (Incorrect - D)

Tests knowledge but does not measure practical application.

References:

ISACA CISA Review Manual

NIST 800-53 (Security Awareness and Training)

ISO 27001: Security Awareness Control

最新問題: 831

カードキーや鍵を使ってコンピュータ室などの機密エリアへの物理的なアクセスを制御しようとするに伴うリスクは何ですか？

- A. 許可されていない人物は、管理されたドアが開くのを待ち、許可された人物の後ろから入ってきます。
- B. 組織の緊急時対応計画では、アクセス制御の実践を効果的にテストすることができません。
- C. アクセスカード、鍵、パッドは簡単に複製できるため、制御が容易に侵害される可能性があります。
- D. 権限を失ったユーザーからアクセス権を削除するのは複雑です。

Answer: A ([メッセージを残す](#))

セクション: 情報資産の保護

Explanation:

The concept of piggybacking compromises all physical control established. Choice B would be of minimal concern in a disaster recovery environment. Items in choice C are not easily duplicated. Regarding choice D, while technology is constantly changing, card keys have existed for some time and appear to be a viable option for the foreseeable future.

最新問題: 832

フォローアップ監査の過程で、IS監査担当者は、最初の監査以降、主要な経営陣の一部が交代しており、現在の経営陣が以前に承認した勧告の一部を実施しないことを決定したことを知りました。監査担当者にとって最善の行動は何でしょうか？

- A. 監査委員会の委員長に通知する
- B. 監査マネージャーに通知する。
- C. コントロールを再テストします。
- D. 監査結果をクローズする。

Answer: ([解答を表示する](#))

最新問題: 833

Which of the following would BEST guide an IS auditor when determining an appropriate time to schedule the follow-up of agreed corrective actions for reported audit issues?

- A. Progress updates indicate that the implementation of agreed actions is on track.

- B. Sufficient time has elapsed since implementation to provide evidence of control operation.
- C. Business management has completed the implementation of agreed actions on schedule.
- D. Regulators have announced a timeline for an inspection visit.

Answer: ([解答を表示する](#))

Explanation

This is because the follow-up of agreed corrective actions for reported audit issues should be done after the auditee has had enough time to implement the corrective actions and demonstrate their effectiveness and sustainability. The follow-up audit should not be too soon or too late, but based on a reasonable and realistic timeframe that allows for adequate testing and verification of the control operation¹².

Answer A. Progress updates indicate that the implementation of agreed actions is on track. is not the best answer, because progress updates are not sufficient to guide the follow-up audit timing. Progress updates are useful for monitoring and communicating the status and challenges of the corrective actions, but they do not provide conclusive evidence of the control operation. The follow-up audit should be based on actual results and outcomes, not on expectations or projections¹².

Answer C. Business management has completed the implementation of agreed actions on schedule. is not the best answer, because the completion of the implementation of agreed actions is not enough to guide the follow-up audit timing. The completion of the implementation only indicates that the auditee has taken the necessary steps to address the audit issues, but it does not guarantee that the corrective actions are effective and sustainable. The follow-up audit should be based on the evaluation and validation of the control operation, not on the completion of the control implementation¹².

Answer D. Regulators have announced a timeline for an inspection visit. is not the best answer, because the regulators' inspection visit is not relevant to guide the follow-up audit timing. The regulators' inspection visit is an external factor that may or may not coincide with the internal follow-up audit schedule. The follow-up audit should be based on the internal audit plan and objectives, not on the external audit requirements or expectations¹².

最新問題: 834

An organization is disposing of removable onsite media which contains sensitive information. Which of the following is the MOST effective method to prevent disclosure of sensitive data?

- A. Software formatting
- B. Encrypting and destroying keys
- C. Machine shredding
- D. Wiping and rewriting three times

Answer: C ([メッセージを残す](#))

最新問題: 835

永続的に重要な電子情報が、長期にわたってアクセス可能な状態を維持することを最も確実に保証するのは、次のうちどれでしょうか？

- A. データを定期的に最新技術に移行する
- B. 古いハードウェアの予防保守を実施する
- C. 古いソフトウェアをエミュレートするアプリケーションを取得する
- D. アーカイブデータの定期的なバックアップ

Answer: ([解答を表示する](#))

最新問題: 836

ITガバナンスを効果的に実施するために、以下のうちどれが最も重要ですか？

- A. 強力なリスク管理体制
- B. 内部監査人のコミットメント
- C. 協力的な企業文化
- D. 文書化されたポリシー

Answer: C ([メッセージを残す](#))

説明

ITガバナンスを効果的に実施するための最も重要な要素は、支援的な企業文化です。支援的な企業文化とは、ITガバナンスプロセスに関わるすべてのステークホルダー間の協力、コミュニケーション、そしてコミットメントを促進する文化です。また、組織全体でITガバナンスに関する共通のビジョン、価値観、目標を共有する文化でもあります。強力なリスク管理の実践、内部監査人のコミットメント、文書化されたポリシーはITガバナンスの実施において重要な要素ですが、支援的な企業文化がなければ十分ではありません。参考文献 :ISACA、CISAレビューマニュアル、第27版、2018年、41ページ

最新問題: 837

効果的な情報セキュリティガバナンスの観点から、価値提供の主な目的は以下のとおりです。

- A. 事業目標を支援するセキュリティ投資を最適化する。
- B. 標準的なセキュリティ対策を実施する。
- C. 標準規格に基づいた解決策を導入する。
- D. 継続的改善の文化を導入する。

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

効果的な情報セキュリティガバナンスにおいては、ビジネス目標を支援するセキュリティ投資の最適化を確実にするために、価値提供が実施されます。価値提供を実現するためのツールと手法には、標準的なセキュリティ対策の導入、標準ベースのソリューションの制度化とコモディティ化、そしてセキュリティを単なる事象ではなくプロセスとして捉える継続的改善文化の導入などが含まれます。

最新問題: 838

Which of the following attacks could capture network user passwords?

- A. Data diddling
- B. Sniffing
- C. IP Spoofing
- D. Surfing

Answer: ([解答を表示する](#))

Section: Information System Operations, Maintenance and Support

Explanation:

A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.

Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap-a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therefore, if the username/ password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:

Data did dlinginvolves changing data before, as it is entered into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Surfing would refer to the surf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

Reference:

CISA Review manual 2014 Page number 321

Official ISC2 Guide to the CISSP 3rd edition Page Number 153

最新問題: 839

分散ネットワークを持つ国税庁は、毎年年末近くに地域事務所へのトラフィックが急増するため、サービス障害が発生しています。この繁忙期にサーバーのパフォーマンスを向上させるために、次のうちどれが最も効果的でしょうか？

- A. 仮想ファイアウォール
- B. プロキシサーバー
- C. ロードバランサー
- D. 仮想プライベートネットワーク (VPN)

Answer: C ([メッセージを残す](#))

説明

ロードバランサーとは、サーバーファーム内の複数のサーバー間で受信ネットワークトラフィックを分散し、サーバーへの負荷過多を防ぎ、システムのパフォーマンスを最適化するツールまたはアプリケーションです。1. ロードバランサーは、利用可能なサーバー間でワークロードを分散し、サービスの中断を防ぐことで、地域オフィスへの大量のトラフィック流入に対処するのに役立ちます。また、サーバーが利用不能になった場合にトラフィックをオンラインサーバーに再ルーティングすることで、高可用性と耐障害性も提供できます。2.

仮想ファイアウォールとは、ソフトウェアベースのファイアウォールであり、仮想ネットワークまたは環境を不正アクセスや悪意のある攻撃から保護します。仮想ファイアウォールは組織のネットワークのセキュリティを強化できますが、サーバーのパフォーマンスを向上させるものではありません。

プロキシサーバーは、クライアントと宛先サーバー間のゲートウェイとして機能する中間サーバーであり、クライアントのIPアドレスを隠蔽し、キャッシュ機能とフィルタリング機能を提供します。プロキシサーバーは、組織ネットワークのセキュリティとプライバシーを向上させることができますが、サーバーのパフォーマンスを向上させるものではありません。

仮想プライベートネットワーク (VPN) とは、インターネットなどの公共ネットワークを介して2台以上のデバイス間で安全な接続を確立するものです。VPNはネットワーク上で送信されるデータを暗号化して保護できますが、機関のサーバーのパフォーマンスを向上させるものではありません。

最新問題: 840

An organization has contracted with a third party to implement and configure a new accounting application. Once the application is implemented, in-house staff will provide all application support and maintenance. Which of the following is MOST important to the success of this initiative?

- A. Ensuring the third party completed testing
- B. Documenting an implementation plan
- C. Conducting a post-implementation review
- D. Establishing a knowledge transfer plan

Answer: ([解答を表示する](#))

最新問題: 841

Which of the following cloud computing models should an organization adopt if faced with challenges in capacity planning and software maintenance?

- A. Platform as a Service (PaaS)
- B. Infrastructure as a Service (IaaS)
- C. Service-oriented architecture
- D. Hybrid cloud model

Answer: A ([メッセージを残す](#))

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 842

技術の変化の速度は、以下の重要性を高めます。

- A. IS機能を外部委託する。
- B. 適切なプロセスを導入し、徹底する。
- C. 組織内でキャリアを築きたいと考えている人材を採用します。
- D. ユーザーの要求を満たす。

Answer: B ([メッセージを残す](#))

変化に対応するには、適切な変更管理プロセスを導入し、徹底する必要があります。情報システム (IS) 機能のアウトソーシングは、技術変化の速度とは直接関係がありません。一般的なIS部門の従業員は高度な資格と教育を受けており、通常は自分の仕事が危ういとは感じておらず、頻繁に転職する用意があります。ユーザー要件を満たすことは重要ですが、IS環境における技術変化の速度とは直接関係がありません。

最新問題: 843

従業員を対象に実施したフィッシングシミュレーションテストの有効性を監査する際、IS監査担当者が最も懸念すべき所見は次のうちどれでしょうか？

- A. 試験に不合格だった職員は、フォローアップ教育を受けなかった。
- B. 検査結果は職員に伝えられなかった。
- C. 職員には事前に検査について通知されていませんでした。
- D. 試験前にセキュリティ意識向上トレーニングは実施されませんでした。

Answer: A (メッセージを残す)

IS監査担当者が最も懸念すべき点は、フィッシングシミュレーションテストに不合格となった職員に対するフォローアップ教育の不足です。フィッシングシミュレーションテストは、職員のフィッシング攻撃に対する認識レベルと脆弱性を評価し、セキュリティ行動を改善するためのフィードバックとトレーニングを提供することを目的としています。テストに不合格となった職員がフォローアップ教育を受けなければ、自らの過ちから学ぶことができず、実際のフィッシング攻撃の被害に遭い続ける可能性があります。組織のセキュリティが危険にさらされる恐れがあります。

その他の選択肢は、IS監査担当者にとってそれほど懸念事項ではない。

* テスト結果はスタッフに伝えられませんでした。スタッフは自身のパフォーマンスに関するフィードバックを受け、テスト結果から学ぶべきであるため、これは理想的ではありません。しかし、これは必ずしもスタッフがフィッシング攻撃を回避する方法に関するトレーニングや教育を受けていないことを意味するものではありません。

* スタッフには事前にテストについて通知されていませんでした。これはフィッシングシミュレーションテストでは一般的な手法であり、スタッフがいつフィッシングメールを受け取るか分からないという現実の状況を再現するものです。このテストの目的は、スタッフの準備状況やコンプライアンスではなく、自発的な反応と認識力を測定することです。

* テスト実施前にセキュリティ意識向上トレーニングは実施されませんでした。しかし、このテストは従業員の現在の意識レベルと脆弱性を測る基準値として機能し、テスト結果に基づいて個別のトレーニングや教育を提供する出発点となるため、これは大きな問題ではありません。

最新問題: 844

Which of the following observations should be of GREATEST concern to an IS auditor reviewing a large organization's virtualization environment?

- A. A rootkit was found on the host operating system
- B. Host inspection capabilities have been disabled
- C. Guest tools have been installed without sufficient access control,
- D. Guest tools have been installed without sufficient access control,
- E. A rootkit was found on the host operating system
- F. Host inspection capabilities have been disabled
- G. An unused printer has been left connected to the host system.

H. An unused printer has been left connected to the host system.

Answer: D ([メッセージを残す](#))

最新問題: 845

An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor's GREATEST concern?

- A. 事業継続計画 (BCP)が更新されていませんでした。
- B. ユーザーは新しいシステムに関するトレーニングを受けていません。
- C. モバイル端末は暗号化されていません。
- D. ユーザーは更新された利用規約に署名する必要はありません。

Answer: A ([メッセージを残す](#))

最新問題: 846

以下のネットワーク構成オプションのうち、任意の2台のホストマシン間に直接リンクが含まれているのはどれですか？

- A. バス
持つてくる
- B. スター
- C. 完全接続 (メッシュ)

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

完全に接続されたメッシュ構成では、任意の2台のホストマシン間に直接リンクが作成されます。

不正解：

- A. バス構成では、1本の送電線に沿って全ての駅が接続されます。
- B. リング構成は円を形成し、すべてのステーションは送信円上の点に接続されます。
- D. スター型構成では、各ステーションはメインハブに直接接続されます。

最新問題: 847

データベースに接続されたアプリケーションの移植性を確保するために役立つのは、次のうちどれですか？

- A. データベースのインポートおよびエクスポート手順の検証
- B. 構造化照会言語 (SQL)の使用
- C. ストアドプロシージャ／トリガーの分析
- D. エンティティ関係モデルとデータベース物理スキーマの同期

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

SQLを使用することで移植性が向上します。他のシステムとのインポートおよびエクスポート手順の検証は、他のシステムとのインターフェースの改善に役立ち、ストアドプロシージャ/トリガーの分析は適切なアクセス/パフォーマンスを保証し、設計エンティティ関係モデルのレビューは役立ちますが、これらのいずれもデータベースに接続するアプリケーションの移植性には貢献しません。

最新問題: 848

データウェアハウス (DW) 管理において、ソースシステムからの変更によって引き起こされるデータ品質の問題を防止するための最善の方法は何ですか？

- A. ソースシステムの変更による影響分析にデータウェアハウスを含める
- B. データウェアハウスとソースシステム間の差異をチェックするためのデータ品質アラートを設定します。
- C. 2つのシステム間での抽出／転送／ロード (ETL) プロセスの変更へのアクセスを制限する
- D. 2つのシステム間の抽出／転送／ロード (ETL) プロセスの変更には承認が必要

Answer: ([解答を表示する](#))

最新問題: 849

監査作業の完了後、IS監査担当者は以下のことを行うべきである。

- A. 被監査者との協議に先立ち、上級管理職に報告書を提出する。
- B. 監査チームのメンバーに、調査結果の概要を配布する。
- C. 被監査者に対し、初期調査結果を記載した報告書を提供する。
- D. 被監査者と作業書類を確認する。

Answer: ([解答を表示する](#))

監査作業の完了後、IS監査人は監査チームのメンバーに監査結果の概要を配布する必要があります。これは、監査チームのメンバーが監査結果を認識し、フィードバックを提供する機会を持ち、監査の結論と勧告について合意できるようにするためです。被監査企業との協議前に上級管理職に報告書を提出すること、被監査企業に初期調査結果を記載した報告書を提出すること、被監査企業と作業文書を確認することは、監査の独立性、客観性、および品質を損なう可能性があるため、IS監査人が監査作業完了後に取りべき適切な行動ではありません。参考文献 :ISACA CISAレビューマニュアル第27版、221ページ

最新問題: 850

ある組織が買収を計画しており、対象企業のITガバナンスフレームワークを評価するためにIS監査人を雇いました。フレームワークの有効性を判断する上で、次のうちどれが最も役立つでしょうか？

- A. 競合他社とのITパフォーマンスベンチマークレポート
- B. IT能力と成熟度に関する販売評価レポート
- C. 最近の第三者機関によるIS監査報告書
- D. 現在および過去の内部IS監査報告書

Answer: C ([メッセージを残す](#))

最新問題: 851

シングルサインオン (SSO) の主な利点は次のうちどれですか？

- A. 適切なパスワード管理を保証します
- B. セキュリティの向上
- C. システムパフォーマンスを向上させます
- D. 事務作業の負担を軽減します

Answer: ([解答を表示する](#))

最新問題: 852

以下の侵入検知システム (IDS) のうち、通常のネットワーク活動によって誤報が発生する可能性が最も高いのはどれですか？

- A. 統計に基づく
- B. 署名ベース
- C. ニューラルネットワーク
- D. ホストベース

Answer: A ([メッセージを残す](#))

統計ベースのIDSは、システムの既知の動作と想定される動作の定義に依存します。通常のネットワークアクティビティには、予期しない動作（たとえば、複数のユーザーによる突然の大量ダウンロード）が含まれる場合があるため、これらのアクティビティは疑わしいものとしてフラグ付けされます。シグネチャベースのIDSは、ウイルススキャナと同様に、事前に定義された検出ルールセットに限定されます。ニューラルネットワークは、上記の2つのIDSを組み合わせて、ハイブリッドでより優れたシステムを作成します。ホストベースは、IDSのもう1つの分類です。上記の3つのIDSはいずれも、ホストベースまたはネットワークベースである可能性があります。

最新問題: 853

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

- A. An increased number of people using technology
- B. Significant cost savings, through a reduction in the complexity of information technology
- C. A weaker organizational structures and less accountability
- D. Increased information protection (IP) risk will increase

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern.

Incorrect answers:

- B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.
- D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

最新問題: 854

大規模システムアップグレード後の導入後レビューを実施するIS監査担当者にとって、以下のうちどれが最も懸念すべき事項でしょうか？

- A. 変更は開発グループによって製品化に向けて推進されます。
- B. オブジェクトコードは開発グループがアクセスできます。
- C. 変更承認は正式には文書化されていません。
- D. 開発者はテスト環境にアクセスできます。

Answer: A ([メッセージを残す](#))

最新問題: 855

リスク評価を実施する主な理由は次のうちどれですか？

- A. 現在のリスクプロファイルを判断する
- B. 事業影響分析 (BIA) との整合性を確保する
- C. 規制要件への準拠を達成するため
- D. リスク軽減策のための予算配分を支援する

Answer: ([解答を表示する](#))

リスク評価を実施する主な理由は、組織の現在のリスクプロファイル、すなわちリスクへの曝露レベル、潜在的な脅威の発生確率および影響度を把握することです。これにより、組織は対処すべきリスクを特定して優先順位を付け、リスク管理戦略を事業目標に整合させることができます。リスク評価は、コンプライアンスの達成、事業影響度分析 (BIA) のサポート、予算配分にも役立ちますが、これらは主な理由ではありません。参考文献 :ISACA用語集、 「リスク評価」の項

最新問題: **856**

組織の品質管理 (QC) プロセスを管理する能力にとって、以下のうちどれが最も大きなリスクとなるか？

- A. 職務分担の欠如
- B. 専用の品質管理機能の欠如
- C. 方針と手順の欠如
- D. 正式な研修や証明書の不足

Answer: ([解答を表示する](#))

説明

組織が品質管理 (QC) プロセスを管理する能力にとって最大の脅威は、QCの目的、基準、方法、役割、責任を明確に定義する方針と手順が欠如していることです。方針と手順がなければ、QCプロセスは一貫性を欠き、効果がなく、非効率的であったり、関連する規制やベストプラクティスに準拠していなかったりする可能性があります。方針と手順は、QCプロセスの基盤と指針を提供し、その品質、信頼性、説明責任を確保するのに役立ちます。

参考文献

ISACA CISAレビューマニュアル、第27版、253ページ

品質管理の概要 | ScienceDirect Topics

品質管理：意味 重要性、定義、目的

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: **857**

Which of the following would provide an IS auditor with the GREATEST assurance that data disposal controls support business strategic objectives?

- A. Media sanitization policy
- B. Media recycling policy
- C. Media shredding policy

D. Media labeling policy

Answer: ([解答を表示する](#))

最新問題: 858

ネットワーク構成の監査を計画する際、IS監査担当者は次のネットワーク文書のうちどれを入手することを最優先事項とすべきでしょうか？

A. 配線図と回路図

B. ユーザーリストと責任

C. アプリケーション一覧とその詳細

D. バックアップと復旧の手順

Answer: A ([メッセージを残す](#))

ネットワーク監査を実施するには、ネットワークの配線図と回路図が必要です。配線図と回路図がない場合、ネットワーク監査は実施できない可能性があります。その他の文書は重要ですが、必須ではありません。

最新問題: 859

Which of the following software development methodology is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems?

A. Agile Developments

B. Software prototyping

C. Rapid application development

D. Component based development

Answer: D ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Component-based software engineering (CBSE) (also known as component-based development (CBD)) is a branch of software engineering that emphasizes the separation of concerns in respect of the wide- ranging functionality available throughout a given software system. It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long- term for the software itself and for organizations that sponsor such software.

Software engineers[who?] regard components as part of the starting platform for service-orientation.

Components play this role, for example, in web services, and more recently, in service-oriented architectures (SOA), whereby a component is converted by the web service into a service and subsequently inherits further characteristics beyond that of an ordinary component.

Components can produce or consume events and can be used for event-driven architectures (EDA).

Definition and characteristics of components

An individual software component is a software package, a web service, a web resource, or a module that encapsulates a set of related functions (or data).

All system processes are placed into separate components so that all of the data and functions inside each component are semantically related (just as with the contents of classes). Because of this principle, it is often said that components are modular and cohesive.

With regard to system-wide co-ordination, components communicate with each other via interfaces. When a component offers services to the rest of the system, it adopts a provided interface that specifies the services that other components can utilize, and

how they can do so. This interface can be seen as a signature of the component - the client does not need to know about the inner workings of the component (implementation) in order to make use of it. This principle results in components referred to as encapsulated. The UML illustrations within this article represent provided interfaces by a lollipop-symbol attached to the outer edge of the component.

However, when a component needs to use another component in order to function, it adopts a used interface that specifies the services that it needs. In the UML illustrations in this article, used interfaces are represented by an open socket symbol attached to the outer edge of the component.

A simple example of several software components - pictured within a hypothetical holiday-reservation system represented in UML 2.0.

Another important attribute of components is that they are substitutable, so that a component can replace another (at design time or run-time), if the successor component meets the requirements of the initial component (expressed via the interfaces). Consequently, components can be replaced with either an updated version or an alternative without breaking the system in which the component operates.

As a general rule of thumb for engineers substituting components, component B can immediately replace component A, if component B provides at least what component A provided and uses no more than what component A used.

Software components often take the form of objects (not classes) or collections of objects (from object- oriented programming), in some binary or textual form, adhering to some interface description language (IDL) so that the component may exist autonomously from other components in a computer.

When a component is to be accessed or shared across execution contexts or network links, techniques such as serialization or marshalling are often employed to deliver the component to its destination.

Reusability is an important characteristic of a high-quality software component. Programmers should design and implement software components in such a way that many different programs can reuse them.

Furthermore, component-based usability testing should be considered when software components directly interact with users. It takes significant effort and awareness to write a software component that is effectively reusable. The component needs to be:

fully documented

thoroughly tested

robust - with comprehensive input-validity checking

able to pass back appropriate error messages or return codes

designed with an awareness that it will be put to unforeseen uses

The following were incorrect answers:

Agile Development - Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.

Reference:

CISA review manual 2014 Page number 194

最新問題: 860

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- A. Install the vendor's security fix for the vulnerability.
- B. Block the protocol traffic in the perimeter firewall.
- C. Block the protocol traffic between internal network segments.
- D. Stop the service until an appropriate security fix is installed.

Answer: D ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

最新問題: 861

以下のリスクシナリオのうち、データ損失防止 (DLP) ツールを使用することで最も効果的に軽減できるのはどれですか？

- A. 従業員が生産性向上のため、社内文書を外部メールアドレスに送信している。
- B. 元従業員が、シングルサインオン (SSO) で認証を行うアプリケーションへのアクセス権を保持している。
- C. 従業員がテスト環境で本番データを使用する
- D. 従業員が書類のデータ分類を誤って選択した

Answer: A ([メッセージを残す](#))

データ損失防止 (DLP) ツールは、機密データの組織外への不正な共有や転送を監視、検知、防止するように設計されています。従業員が意図的または意図せずに会社の文書を外部のメールアドレスに送信してしまうような、データ漏洩のリスクを軽減するのに最適です。

最新問題: 862

IS監査業務を計画する際に、リスク評価を実施する際の主要な目的は何でしょうか？

- A. 高リスクな業務プロセスを特定する
- B. 必要な実質的試験のレベルを最小限に抑えるため
- C. リスクを許容できるレベルまで低減する
- D. 業務に割り当てられたリソースの数を最小限に抑える

Answer: (解答を表示する)

最新問題: 863

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- A. Degaussing
- B. Overwrite every sector of magnetic media with pattern of 1's and 0's

C. Format magnetic media

D. Delete File allocation table

Answer: A (メッセージを残す)

Explanation/Reference:

PERMANENTLY is the keyword used in the question. You need to find out data removal method which remove data permanently from magnetic media.

Degaussing is the most effective method out of all provided choices to erase sensitive data on magnetic media provided magnetic media is not require to be reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed.

Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides.

Specialized hardware devices known as degausses can be used to erase data saved to magnetic media.

The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist.

Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives.

The security professional should exercise caution when recommending or using degausses on media for reuse.

Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There is a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time.

The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten.

この場合、より高い安全性を確保するためには、各セクターを複数回上書きする必要があります。セキュリティ担当者は、重要度の低い情報であれば1回の上書きで十分な場合がありますが、機密性の高いデータは複数回上書きする必要があることを念頭に置いておくべきです。上書きソフトウェアは、USBメモリなどのソリッドステートメディア内のセクターを消去するためにも使用できます。使用しなくなったソリッドステートメディアについては、焼却や安全なリサイクルなどの物理的な破壊方法を検討することをお勧めします。

機密データへの不正アクセスを防止する最後の手段は、メディアの破壊です。シュレッダー処理、焼却、粉碎、粉末化は、メディアを物理的に破壊する一般的な方法です。消磁もメディア破壊の一形態です。高出力の消磁器は、場合によってはハードディスクのプラッタを文字通り曲げたり歪ませたりするほど強力です。

細断と焼却は、非剛性磁気メディアの有効な破壊方法です。実際、一部のシュレッダーは光ディスクなどの剛性メディアも細断できます。ディスクを機械に投入した後、残る残渣のサイズが小さいため、機密性の低い情報を含む光メディアであれば、これは有効な代替手段となり得ます。

しかし、機密情報を含むメディアの場合、残留物のサイズが大きすぎる可能性があります。代わりに、リジッドメディアやソリッドステートメディアには、研削や粉碎が適切な選択肢となります。光メディアの表面を研削するための専用装置があり、表面を十分に傷つけて読み取り不能にするか、ディスクのデータ層を実際に削り取ります。ドライブを回収し、依頼に応じて現場で破壊し、完了証明書を発行するサービスもいくつか存在します。メディアの洗浄と廃棄に関して、最も適切なソリューションを選択、維持、支援するのは、セキュリティ専門家の責任となります。

以下の回答は誤りです。

磁気媒体のすべてのセクターを1と0のパターンで上書きする - 磁気媒体を再利用する必要がある場合は、消磁よりも効果が低い。

磁気メディアのフォーマット - 磁気メディアをフォーマットしても、すべてのデータが消去されるわけではありません。フォーマット後でも、ソフトウェアツールを使用すればデータを復元できます。

ファイル割り当てテーブルを削除しても、すべてのデータが消去されるわけではありません。ソフトウェアツールを使用すれば、データを復元できる場合があります。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 338ページ

ISC2公式CISSP CBKガイド第3版、720ページ。

最新問題: 864

組織は、従業員からの電子メールの受信者が送信者の身元を認証できるようにするために、以下の方法を用いることができます。

- A. すべての電子メールメッセージにデジタル署名を行う。
- B. すべての電子メールメッセージを暗号化する。
- C. すべての電子メールメッセージを圧縮します。
- D. すべての電子メールメッセージにパスワード保護をかける。

Answer: A (メッセージを残す)

セクション：情報資産の保護

Explanation:

すべての電子メールにデジタル署名を行うことで、受信者は送信者の正当性を検証できるようになります。

すべての電子メールメッセージを暗号化すれば、意図した受信者のみがメッセージを開くことができるようになりますが、送信者の正当性を保証するものではありません。すべての電子メールメッセージを圧縮すれば、メッセージのサイズは小さくなりますが、正当性を保証するものではありません。すべての電子メールメッセージにパスワードを設定すれば、パスワードを知っている人だけがメッセージを開くことができるようになりますが、送信者の正当性を保証するものではありません。

最新問題: 865

情報システム監査担当者が、組織構造の変更に伴う業務プロセスへの重大な影響を踏まえ、組織の事業継続計画（BCP）をレビューしています。監査担当者が最も懸念すべき事項は次のうちどれでしょうか？

- A. 主要な業務プロセスのエンドユーザーは、業務影響分析（BIA）に参加しませんでした。
- B. 組織再編以降、BCPのコピーは新しい事業部門のエンドユーザーに配布されていません。
- C. 過去2年間、BCPのテスト計画は完了していません。

Answer: C ([メッセージを残す](#))

BCP（事業継続計画）のテスト計画は、計画が効果的で最新の状態に保たれ、現在の事業ニーズと目標に合致していることを保証するために不可欠です。事業プロセスに大きな影響を与える組織構造の変更は、BCPの改訂と、その妥当性を検証するための新たなテスト計画の策定を必要とする場合があります。2年間BCPのテスト計画がないということは、災害や事業中断が発生した場合に失敗するリスクが高いことを示しています。

したがって、これは提示された選択肢の中で監査人が最も懸念すべき事項である。参考文献：

ISACA、サーベンス・オクスリー法に基づくIT統制目標、第4版、セクション5.3.21 ISACA、CISAレビューマニュアル、第27版、第5章、セクション5.42

最新問題: 866

組織内のデータ分類レベルを定義するのに最も適したエンティティは次のうちどれですか？

- A. データスキーマに基づくデータベース管理者
- B. 申請規則に基づく法務コンプライアンスチーム
- C. 各データに責任を負う事業主
- D. データセキュリティ管理を担当するシステム管理者

Answer: C ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 867

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

- A. Restricting evidence access to professionally certified forensic investigators
- B. Documenting evidence handling by personnel throughout the forensic investigation
- C. Performing investigative procedures on the original hard drives rather than images of the hard drives
- D. Engaging an independent third party to perform the forensic investigation

Answer: B ([メッセージを残す](#))

The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation. Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time, location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the investigation. References:

CISA Review Manual (Digital Version)

CISA Questions, Answers and Explanations Database

最新問題: 868

ITバランススコアカードは、以下の項目以外のITパフォーマンス評価指標を監視することを目的としたビジネスガバナンスツールです。

- A. 財務実績
- B. 顧客満足度
- C. 内部プロセスの効率。
- D. イノベーション能力。

Answer: A ([メッセージを残す](#))

従来、財務実績は唯一の総合的な業績評価指標とされてきました。ITバランススコアカード (BSC)は、財務実績以外のIT業績評価指標を監視することを目的としたITビジネスガバナンスツールです。IT BSCは、顧客満足度、イノベーション能力、処理能力など、その他の重要な成功要因も考慮に入れています。

最新問題: 869

次の攻撃のうち、複数のゲートウェイのブロードキャストアドレスに偽造されたICMPエコー要求パケットを送信し、ゲートウェイの背後にあるコンピュータから応答を不正に引き出し、それらのコンピュータがすべてICMPエコー要求パケットの送信元IPアドレスにICMPエコー応答パケットで応答するという攻撃はどれですか？

- A. 反射攻撃
- B. 力任せの攻撃
- C. バッファオーバーフロー
- D. 脈動するゾンビ

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

リフレクテッド攻撃とは、偽造されたリクエストを多数のコンピュータに送信し、それらのコンピュータがリクエストに応答するように仕向ける攻撃手法です。送信元IPアドレスは標的のコンピュータのIPアドレスに偽装され、応答が大量に発生するように仕向けられます。

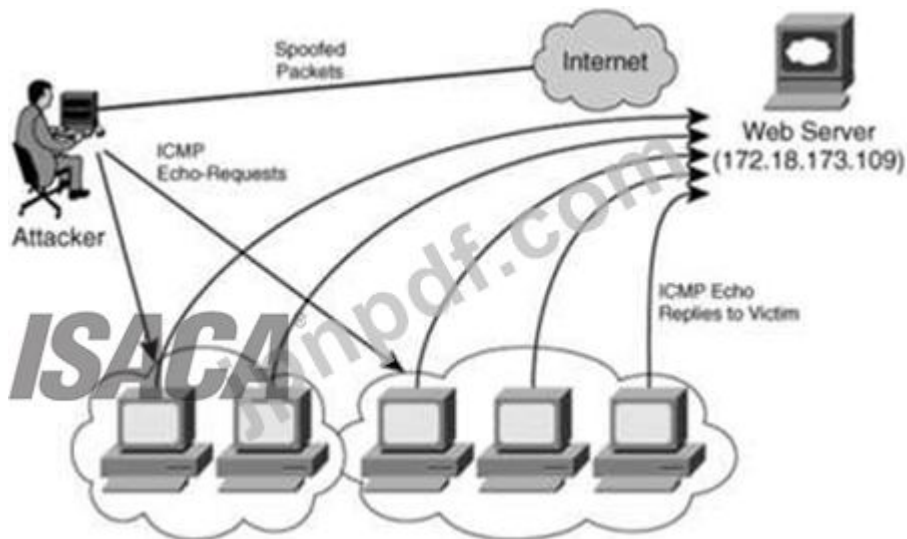
分散型サービス拒否攻撃では、偽造されたリクエストを非常に多数のコンピュータに送信し、それらのコンピュータがリクエストに応答するように仕向けます。インターネットプロトコルアドレスの偽装を用いることで、送信元アドレスを標的のコンピュータのアドレスに設定し、すべての応答が標的のコンピュータに送られ (そして溢れかえる) ことになります。

(この反射型攻撃は「DRDOS」と呼ばれることもあります。)

ICMPエコー要求攻撃 (スマーフ攻撃)は、反射型攻撃の一種とみなすことができます。攻撃側のホストは、構成が混在するネットワークのブロードキャストアドレスにエコー要求を送信し、それによって他のホストに被害者へのエコー応答パケットの送信を促します。初期のDDoS攻撃プログラムの中には、この攻撃の分散型を実装したものもありました。

In the surf attack, the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address. This means that each system on the victim's subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets-which is the victim's address. All of these response packets go to the victim system and overwhelm it because it is being bombarded with packets it does not necessarily know how to process. The victim system may freeze, crash, or reboot. The Smurf attack is illustrated in Figure below:

surf-attack



The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Reference:

CISA review manual 2014 Page number 322

最新問題: 870

Which of the following provides the GREATEST assurance that any confidential information on a disk is no longer accessible but the device is still usable by other internal users?

- A. Reformatting the disk
- B. Erasing the disk
- C. Degaussing the disk
- D. Password-protecting the disk

Answer: A ([メッセージを残す](#))

Section: Protection of Information Assets

最新問題: 871

Which of the following would be an appropriate role of internal audit in helping to establish an organization's privacy program?

- A. Analyzing risks posed by new regulations
- B. Developing procedures to monitor the use of personal data

C. Defining roles within the organization related to privacy

D. 個人データを保護するための制御設計

Answer: (解答を表示する)

組織のプライバシープログラムの確立を支援する上で、内部監査が果たすべき適切な役割の一つは、新たな規制によって生じるリスクを分析することです。プライバシープログラムとは、個人の個人データを不正または違法な収集、使用、開示、廃棄から保護することを目的とした、一連のポリシー、手順、および管理策のことです。

プライバシープログラムは、一般データ保護規則 (GDPR) やカリフォルニア州消費者プライバシー法 (CCPA) など、個人および組織のプライバシー権と義務を規定する適用法令を遵守する必要があります。新たな規制により、組織のプライバシープログラムに影響を与え、コンプライアンス上のリスクや罰則につながる可能性のある新たな要件や変更が導入される場合があります。そのため、内部監査は、新たな規制によって生じるリスクを分析し、それらに対処する方法について保証、助言、または推奨事項を提供することで、組織のプライバシープログラムの確立を支援できます。1. 他の選択肢は、以下の理由から適切または不適切です。

* B. 個人データの使用を監視する手順の開発は、組織のプライバシー プログラムを確立する上で内部監査が果たすべき適切な役割ではありません。これは、管理または運用上の役割に近いからです。内部監査は、組織のプライバシー プログラムの設計や実装に関与すべきではありません。そうすると、その独立性と客観性が損なわれるからです。内部監査は、組織のプライバシー プログラムの効果と効率性について保証を提供するべきであり、作成や実行を行うべきではありません。2.

* C. 組織のプライバシーに関連する役割を定義することは、組織のプライバシープログラムの確立を支援する内部監査の適切な役割ではありません。それは、ガバナンスまたは戦略的な役割に近いからです。

内部監査は、組織のプライバシー戦略、目標、またはポリシーの設定や承認に関与すべきではありません。なぜなら、それは内部監査の独立性と客観性を損なうことになるからです。内部監査は、組織のプライバシープログラムが戦略、目標、およびポリシーと整合し、遵守していることを保証するべきですが、それらを定義したり承認したりすべきではありません。

* D. 個人データを保護するための管理策の設計は、組織のプライバシー プログラムの確立を支援する内部監査の適切な役割ではありません。これは、管理または運用上の役割です。内部監査は、組織のプライバシー プログラムの設計または実装に関与すべきではありません。これは、内部監査の独立性と客観性を損なうためです。内部監査は、組織のプライバシー プログラムの適切性と有効性について保証を提供するべきであり、設計または実装するべきではありません。2. 参考文献: ISACA が事業継続/災害対策のための新しい監査プログラムを導入...、プライバシー監査のベスト プラクティス - ISACA、ISACA がデータ プライバシーと...のための新しい監査および保証プログラムを作成...

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 872

.Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

A. Cold site

B. Hot site

C. Alternate site

D. Warm site

Answer: A ([メッセージを残す](#))

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data .

最新問題: 873

An organization is developing a web portal using some external components. Which of the following should be of MOST concern to an IS auditor?

A. Open-source components were integrated during development.

B. Some of the developers are located in another country.

C. The organization has not reviewed the components for known exploits.

D. Staff require additional training in order to perform code review.

Answer: C ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 874

サーバー上で不審な活動が確認された後、管理者はフォレンジック分析を依頼した。

以下の所見のうち、調査担当者が最も懸念すべきものはどれですか？

A. サーバーはワークグループのメンバーであり、サーバードメインの一部ではありません

B. サーバーでゲストアカウントが有効になっています

C. 最近、サーバーに100人のユーザーが作成されました

D. サーバーで監査ログが有効になっていません

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

監査ログは調査を進める上で必要な証拠を提供する可能性があるため、無効化すべきではありません。業務上の必要性から、サーバーはワークグループのメンバーとなることができ、その場合は問題になりません。

システムにゲストアカウントを有効にしておくことはセキュリティ上の問題ではありますが、フォレンジック調査の対象となるような懸念事項ではありません。最近サーバーに100人のユーザーを作成したのは、業務上のニーズを満たすために必要だった可能性があり、懸念すべき事項ではないでしょう。

最新問題: 875

Which of the following findings would be of GREATEST concern when auditing an organization's end-user computing (EUC)?

A. Errors flowed through to financial statements

B. Inconsistency of patching processes being followed

C. Reduced oversight by the IT department

D. Inability to monitor EUC audit logs and activities

Answer: A ([メッセージを残す](#))

最新問題: 876

次のうち、通常のシステム認証手順を回避する方法を指すのはどれですか？

- A. ウイルス
- B. 虫
- C. トロイの木馬
- D. スパイウェア
- E. ルートキット
- F. バックドア
- G. 選択肢に該当しない。

Answer: F ([メッセージを残す](#))

バックドアとは、通常の認証手順を回避する方法のことである。

多くのコンピュータメーカーは、技術的な利点を提供するために、システムにバックドアを事前にインストールしていました。

顧客サポート。ハッカーは通常、コンピュータへのリモートアクセスを保護するためにバックドアを使用します。

カジュアルな人目を避けて隠れようとしながら

検査。バックドアを仕掛ける際、ハッカーはトロイの木馬かコンピュータワームのどちらかを好んで使う。

最新問題: 877

Which of the following would be a result of utilizing a top-down maturity model process?

- A. A means of benchmarking the effectiveness of similar processes with peers
- B. Identification of older, more established processes to ensure timely review
- C. Identification of processes with the most improvement opportunities
- D. A means of comparing the effectiveness of other processes within the enterprise

Answer: C ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation

最新問題: 878

全社規模のシステム開発における運営委員会の議長として最も適任な人物は誰か？

通常は次のようになるはずです。

- A. プロジェクトマネージャー
- B. ISディレクター
- C. 経営幹部レベルのマネージャー。
- D. ビジネスアナリスト

Answer: (解答を表示する)

セクション：情報資産の保護

最新問題: 879

以下の活動のうち、組織内に存在する可能性のある個人間の依存関係について、IS監査担当者に最も深い洞察を与えるのはどれですか？

- A. 休暇パターンの見直し
- B. ユーザーアクティビティログの確認
- C. IT部門の上級管理職へのインタビュー

D. ITプロセスを役割にマッピングする

Answer: D ([メッセージを残す](#))

説明

ITプロセスを役割にマッピングすることは、組織内に存在する可能性のある、特定の人物のみに依存する状況について、情報システム監査担当者が最も深い洞察を得られる活動です。特定の人物のみに依存する状況とは、重要なIT機能を実行するために必要な知識、スキル、またはアクセス権限を、たった一人の人物しか持っていない場合に発生します。

ITプロセスを役割にマッピングすることで、こうした依存関係を特定し、IT運用の継続性とセキュリティへの影響を評価することができます。他の活動では、ITプロセスと役割の関係が示されないため、個人間の依存関係についてそれほど深い洞察は得られません。参考文献 :CISAレビューマニュアル、第27版、94ページ

最新問題: 880

Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

- A. The job scheduler application has not been designed to display pop-up error
- B. Changes to the job scheduler application's parameters are not approved reviewed by an operations supervisor.
- C. Operations shift turnover logs are not utilized to coordinate and control the processing environment.
- D. Access to the job scheduler application has not been restricted to a maximum of two start members

Answer: B ([メッセージを残す](#))

最新問題: 881

An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

- A. Allow changes to be made only with the DBA user account.
- B. Make changes to the database after granting access to a normal user account.
- C. Use the DBA user account to make changes, log the changes and review the change log the following day.
- D. Use the normal user account to make changes, log the changes and review the change log the following day.

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

The use of a database administrator (DBA) user account is normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

最新問題: 882

業務に必要なメールは、従業員の個人端末に保存されている。
IS監査担当者にとって、次のうち最も適切な推奨事項はどれですか？

- A. 個人用デバイスにウイルス対策ソフトがインストールされていることを確認してください。
- B. 個人用デバイスにメールコンテナ化ソリューションを実装する
- C. 従業員に個人端末でのパスワードの使用を義務付ける
- D. 従業員が会社のメールを個人端末に保存することを禁止する

Answer: ([解答を表示する](#))

最新問題: 883

IS監査担当者は、サービスプロバイダーの監査を実施する際に、サービスプロバイダーが業務の一部を別のプロバイダーにアウトソーシングしていることに気づいた。その業務には機密情報が含まれるため、IS監査担当者が最も懸念すべき事項は次のとおりである。

- A. 情報の機密性を保護するための要件が損なわれる可能性があります。
- B. アウトソーシング業者からの事前の許可が得られなかったため、契約が解除される可能性があります。
- C. 業務を外部委託している他のサービスプロバイダーは監査の対象ではありません。
- D. アウトソーサーは、さらなる作業のために他のサービスプロバイダーに直接連絡します。

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

多くの国が、自国内で保管されている情報や他国と交換される情報の機密性を保護するための規制を制定しています。サービスプロバイダーがサービスの一部を別のサービスプロバイダーにアウトソーシングする場合、情報の機密性が損なわれるリスクがあります。選択肢BとCは懸念事項となる可能性があります、情報の機密性を確保することとは関係ありません。IS監査人が選択肢Dを懸念する理由はありません。

最新問題: 884

The FIRST step in managing the risk of a cyber attack is to:

- A. assess the vulnerability impact.
- B. evaluate the likelihood of threats.
- C. identify critical information assets.
- D. estimate potential damage.

Answer: C ([メッセージを残す](#))

Explanation/Reference:

Explanation:

The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

最新問題: 885

アプリケーションシステム制御の有効性に対する最大のリスクは次のうちどれですか？

- A. 手作業による処理工程の削除

- B. 手順マニュアルが不十分
- C. 従業員間の共謀
- D. 未解決の規制遵守問題

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

共謀は、継続可能な能動的な攻撃であり、綿密に設計されたアプリケーション制御であっても回避される可能性があるため、特定が困難です。その他の選択肢は、適切に設計されたアプリケーション制御には影響を与えません。

最新問題: 886

情報システム部門における職務分掌の最も確実な証拠となる監査手法はどれですか？

- A. 経営陣との話し合い
- B. 組織図の見直し
- C. 観察とインタビュー
- D. ユーザーアクセス権限のテスト

Answer: ([解答を表示する](#)**)**

セクション：情報資産の保護

説明: IS スタッフが業務を遂行している様子を観察することで、IS 監査担当者は、彼らが互換性のない操作を実行すること、およびISスタッフへのインタビューにより、監査人は概要を把握することができます。実行されたタスク。監査人は、観察とインタビューに基づいて、分離を評価できます。職務。経営陣は、IS部門の各従業員の詳細な職務内容を把握していない可能性がある。したがって、経営陣との話し合いでは分離に関する限られた情報しか得られないだろう。職務。組織図では従業員の職務の詳細が示されません。ユーザーテスト権利はISシステム内での権利に関する情報を提供するが、それらが果たす機能に関する完全な情報。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 887

An IS auditor is evaluating an organization's IT strategy and plans. Which of the following would be of GREATEST concern?

- A. There is not a defined IT security policy.
- B. The business strategy meeting minutes are not distributed.
- C. IT is not engaged in business strategic planning.
- D. There is inadequate documentation of IT strategic planning.

Answer: C ([メッセージを残す](#))

Explanation

The greatest concern for an IS auditor when evaluating an organization's IT strategy and plans is that IT is not engaged in business strategic planning, as this indicates a lack of alignment between IT and business objectives, which could result in inefficient and ineffective use of IT resources and capabilities. The absence of a defined IT security policy, the nondistribution of business strategy meeting minutes, and the inadequate documentation of IT strategic planning are also issues that should be addressed by an IS auditor, but they are not as significant as IT's noninvolvement in business strategic planning. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.1

最新問題: 888

Which of the following should be an IS auditor's PRIMARY focus when evaluating the response process for cybercrimes?

- A. Communication with law enforcement
- B. Notification to regulators
- C. Root cause analysis
- D. Evidence collection

Answer: (解答を表示する)

Evidence collection is the process of identifying, acquiring, preserving, and documenting digital evidence from various sources, such as computers, networks, mobile devices, or cloud services, that can be used to support the investigation and prosecution of cybercrimes. Evidence collection is an IS auditor's primary focus when evaluating the response process for cybercrimes, because it determines the quality and validity of the evidence that can be used to prove or disprove the facts of the case, identify the perpetrators, and recover the losses. Evidence collection should follow the standards and best practices for digital forensics, such as ISO

/IEC 270371, which provide guidelines for ensuring the integrity, authenticity, reliability, and admissibility of the evidence2.

The other possible options are:

- * A. Communication with law enforcement: This is the process of reporting, cooperating, and coordinating with law enforcement agencies that have the jurisdiction and authority to investigate and prosecute cybercrimes. Communication with law enforcement is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Communication with law enforcement depends on the legal and regulatory requirements, the nature and severity of the incident, and the organizational policies and procedures. Communication with law enforcement should be done after evidence collection, to avoid compromising or contaminating the evidence3.
- * B. Notification to regulators: This is the process of informing and updating the relevant regulatory bodies or authorities that oversee or supervise the organization's activities or industry sector about the cybercrime incident. Notification to regulators is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Notification to regulators depends on the legal and regulatory requirements, the nature and impact of the incident, and the organizational policies and procedures. Notification to regulators should be done after evidence collection, to avoid disclosing sensitive or confidential information4.
- * C. Root cause analysis: This is the process of identifying and analyzing the underlying factors or causes that led to or contributed to the cybercrime incident. Root cause analysis is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Root cause analysis helps to prevent or mitigate future incidents, improve security controls and processes, and learn from mistakes. Root cause analysis should be done after evidence collection, to avoid interfering with or affecting the investigation5.

最新問題: 889

メッセージの機密性を確保する制御を監査およびテストする際に、IS監査担当者がWAPゲートウェイを特に重視し、レビューする必要があるのはなぜですか？

- A. WAPはデフォルト設定で構成されていることが多く、そのためセキュリティが脆弱です。
- B. WAPは無線トラフィックに対して弱い暗号化を提供します。
- C. WAPは、無線TLSからインターネットSSLへのプロトコル変換ゲートウェイとして機能します。
- D. WAPは重要なITシステムとインターフェースすることが多い。

Answer: C ([メッセージを残す](#))

無線TLSからインターネットSSLへのプロトコル変換ゲートウェイとして機能するWAPゲートウェイは、メッセージの機密性を確保する制御を監査およびテストする際に、IS監査担当者が特に注意を払い、確認すべきコンポーネントです。

最新問題: 890

ゼロデイ攻撃の検出を最も容易にするのは、次のうちどれですか？

- A. 侵入検知システム (IDS)
- B. ユーザー行動分析
- C. 侵入防御システム (IPS)
- D. マルウェア対策ソフトウェア

Answer: B ([メッセージを残す](#))

説明

ゼロデイ攻撃は検出が非常に困難な場合が多い。マルウェア対策ソフトウェアや一部の侵入検知システム (IDS)、侵入防御システム (IPS)は、攻撃シグネチャがまだ存在しないため、効果を発揮しないことが多い。そのため、ゼロデイ攻撃を検出する最善の方法は、ユーザー行動分析である。

最新問題: 891

Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

- A. DTE
- B. DCE
- C. DME
- D. DLE

Answer: B ([メッセージを残す](#))

Section: Information System Operations, Maintenance and Support

Explanation:

Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

For your exam you should know below information about WAN Technologies:

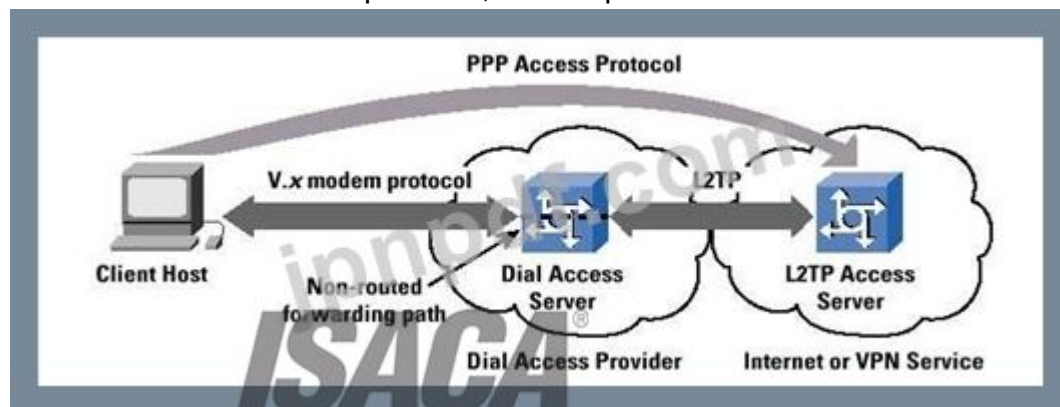
Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested

Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.



Point-to-point protocol

X.25

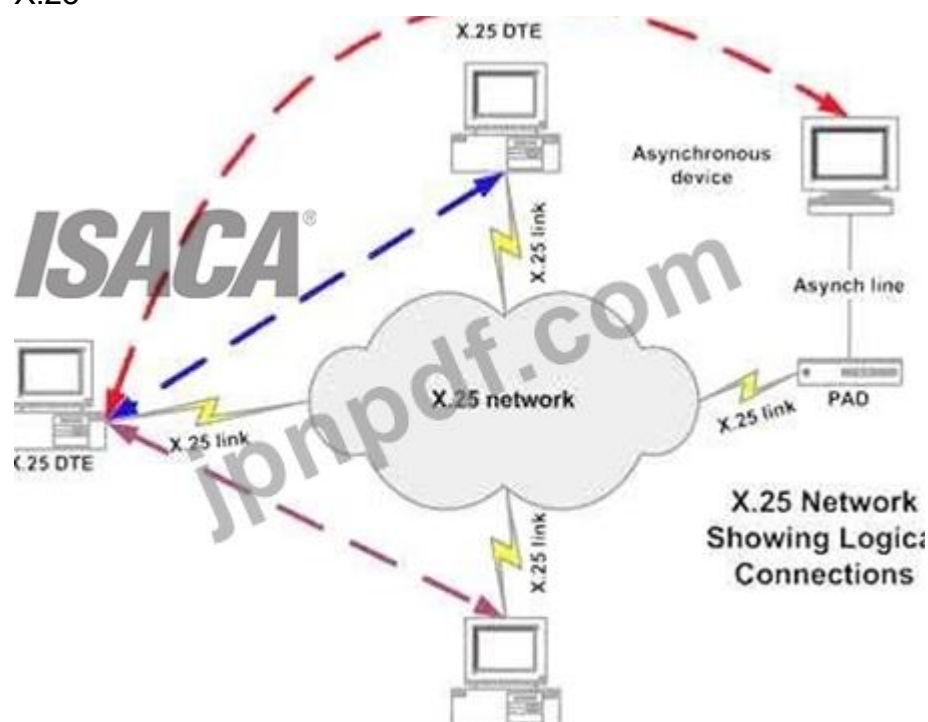
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

X.25



Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Two main types of equipments are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.
2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality.

Frame relay is any to any service.

Frame Relay

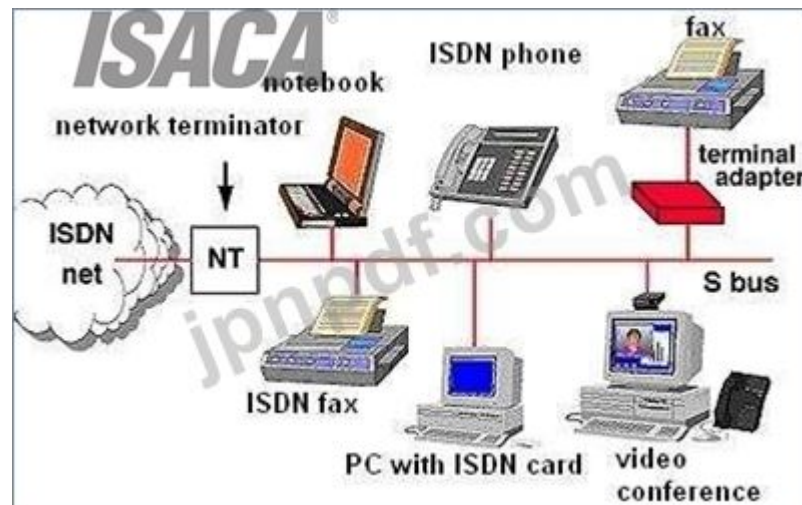
Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium

ISDN

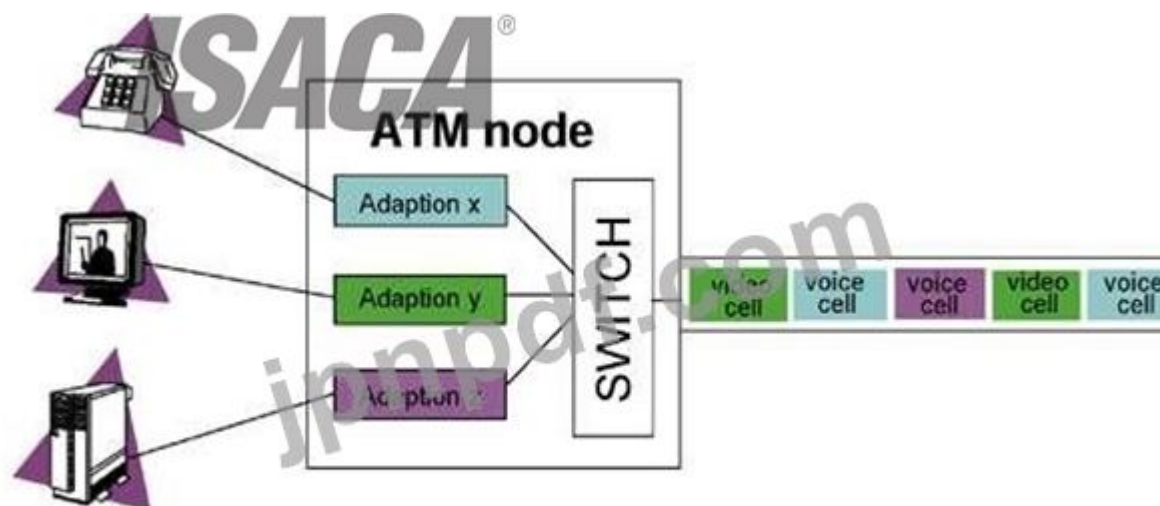


Asynchronous Transfer Mode (ATM)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel Data are segmented into fixed size cell of 53 bytes Some companies have replaces FDDI back-end with ATM Asynchronous Transfer Mode

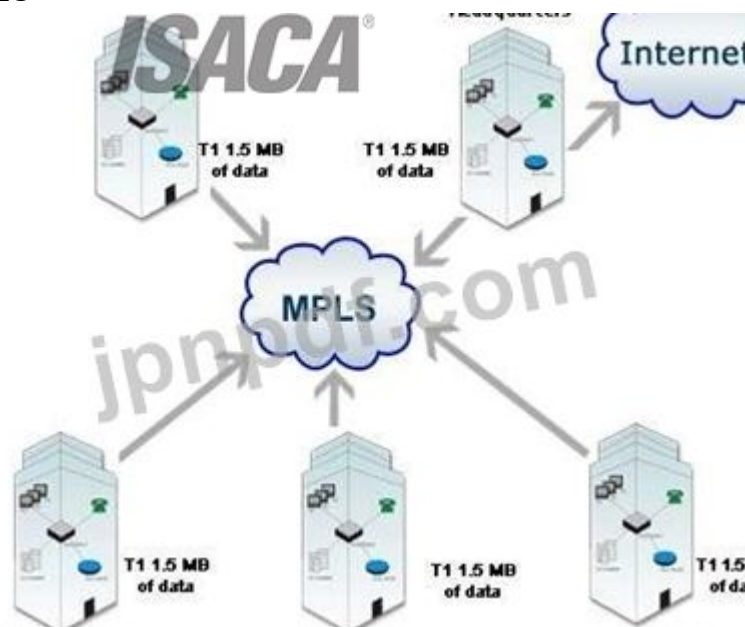


Services	Adaptation layer	ATM layer	Physical Layer

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

DTE - Data Terminal Equipment (DTE) is usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

DME - Not a valid frame relay technique

DLE - Not a valid frame relay technique

Reference:

CISA review manual 2014 page number 266

最新問題: 892

Which of the following is MOST important when creating a forensic image of a hard drive?

- A. Requiring an independent third-party be present while imaging
- B. Choosing an industry-leading forensics software tool
- C. Securing a backup copy of the hard drive
- D. Generating a content hash of the hard drive

Answer: ([解答を表示する](#))

最新問題: 893

組織がリカバリポイント目標 (RPO) で定義された非常に詳細なデータ復元ポイントを必要とする場合、以下のバックアップ手法のうちどれが最も適切でしょうか？

- A. 仮想テープライブラリ
- B. デスクベースのスナップショット
- C. 継続的なデータバックアップ
- D. ディスクからテープへのバックアップ

Answer: C ([メッセージを残す](#))

説明／参考資料：

Explanation:

リカバリポイント目標 (RPO) は、障害発生時に許容できるデータ損失量に基づいて設定されます。このシナリオでは、組織は短いRPOを必要とします。仮想テープライブラリ、デスクベースのスナップショット、ディスクからテープへのバックアップは、バックアップ完了までに時間がかかりますが、継続的なデータバックアップはオンライン (リアルタイム) で行われます。

最新問題: 894

社内ヘルプデスクの手順がポリシーに準拠して実行されていることを確認するための最適な方法は、次のうちどれですか？

- A. ヘルプデスクの通話指標を評価する。
- B. ヘルプデスクの手順をベンチマークする。
- C. エンドユーザーへのインタビュー
- D. クローズされたチケットのサンプルをテストします。

Answer: D ([メッセージを残す](#))

最新問題: 895

すべてのプログラム変更を自動的に報告する環境において、本番プログラムへの不正な変更を検出する最も効率的な方法は次のうちどれですか？

- A. 変更に対するユーザー管理承認の確認
- B. 定期的にテストデータを実行し、本番プログラムと比較検討する
- C. Reviewing the last compile date of production programs
- D. 本番プログラムのコードを管理対象コピーと手動で比較する

Answer: ([解答を表示する](#))

最新問題: **896**

Which of the following is MOST important to review during the project initiation phase of developing and deploying a new application?

- A. Deployment plans
- B. Architectural design
- C. User requirements
- D. User acceptance testing (UAT) plans

Answer: ([解答を表示する](#))

最新問題: **897**

A data administrator is responsible for:

- A. maintaining database system software.
- B. defining data elements, data names and their relationship.
- C. developing physical database structures.
- D. developing data dictionary system software.

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

最新問題: **898**

Which of the following fourth generation language depends on self-contained database management systems?

- A. Query and report generator
- B. Embedded database 4GLs
- C. Relational database 4GL
- D. Application generators

Answer: B ([メッセージを残す](#))

Section: Information System Acquisition, Development and Implementation Explanation:

Embedded database 4GLs are dependent on self-contained database management systems. These characteristics often make them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

For CISA exam you should know below mentioned types of 4GLs

Query and report generator - These specialize language can extract and produce reports. Recently more powerful language has been produced that can access database records, produce complex on-line output and be developed in an almost natural language.

Embedded database 4GLs - These depend on self-contained database management systems. These characteristics often make them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

Relational database 4GLs - These high level language products are usually an optional feature on vendor's DBMS product line. These allow the application developer to make better use of DBMS product, but they often are not end-user-oriented. Example include SQL+ MANTIS and NATURAL.

Application generators - These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.

The following were incorrect answers:

Query and report generator - These specialize language can extract and produce reports.

Relational database 4GLs - These high level language products are usually an optional feature on vendor's DBMS product line.

Application generators - These development tools generate lower level programming languages(3GL) such as COBOL and C.

Reference:

CISA review manual 2014 Page number 209

最新問題: 899

For a discretionary access control to be effective, it must:

- A. operate within the context of mandatory access controls.
- B. operate independently of mandatory access controls.
- C. enable users to override mandatory access controls when necessary.
- D. be specifically permitted by the security policy.

Answer: A ([メッセージを残す](#))

Mandatory access controls are prohibitive; anything that is not expressly permitted is forbidden. Only within this context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. When systems enforce mandatory access control policies, they must distinguish between these and the mandatory access policies that offer more flexibility. Discretionary controls do not override access controls and they do not have to be permitted in the security policy to be effective.

最新問題: 900

監査対象企業がフォローアップ監査の時点までにすべての監査勧告事項を完了できない場合、IS監査担当者取るべき最善の行動は何でしょうか？

- A. 監査結果に未解決の問題が確実に記載されるようにする。
- B. 未解決の問題があるため、フォローアップを終了する
- C. 未解決の問題に対する補償的な管理策を推奨します。
- D. 未解決の問題による残存リスクを評価する。

Answer: D ([メッセージを残す](#))

監査対象者がフォローアップ監査の時点で全ての監査勧告を完了できない場合、IS監査人取るべき最善の行動は、未解決の問題に起因する残存リスクを評価することです。残存リスクとは、統制措置や軽減策の実施後に残るリスクのことです。未解決の問題に起因する残存リスクを評価することで、IS監査人は、監査対象者が対処していない潜在的な脅威や脆弱性の影響と発生可能性、および既存の統制措置や軽減策の適切性と有効性を評価することができます。また、未解決の問題に起因する残存リスクを評価することで、IS監査人は未解決の問題を優先順位付けし、監査対象者や経営陣、監査委員会などの他の利害関係者に伝え、適切な対策やエスカレーション手順を推奨することもできます。

監査対象者がフォローアップ監査の時点までにすべての監査勧告を解決できない場合、IS監査人が未解決の問題を監査結果に残しておくことは一つの対処法ではあるが、最善の方法ではない。

監査結果に未解決事項を記載することで、IS監査担当者は監査勧告の状況と進捗状況を文書化して報告できるだけでなく、今後のフォローアップ監査の基礎資料としても役立ちます。しかし、監査結果に未解決事項を記載するだけでは、意思決定や行動を起こす上でより重要な、未解決事項に起因する残存リスクの分析や評価は得られません。

未解決の問題が解決されていないことを理由にフォローアップを終了することは、被監査企業がフォローアップ監査の時点までにすべての監査勧告を完了できない場合に、IS監査人が取るべき行動ではなく、むしろその結果または成果です。未解決の問題が解決されていないことを理由にフォローアップを終了することは、被監査企業が合意された措置や期限を遵守しなかったこと、またはIS監査人が被監査企業から重大な障害や抵抗に遭遇したことを示している可能性があります。未解決の問題が解決されていないことを理由にフォローアップを終了すると、IS監査人またはその他の当局による、限定付意見や不適正意見の発行、認証の保留、罰則の適用などのさらなる措置や制裁が引き起こされる可能性もあります。

未解決の問題に対する補完的統制の推奨は、被監査企業がフォローアップ監査の時点で全ての監査勧告を完了できない場合にIS監査人が取るべき行動ではなく、むしろその結果として起こりうるものです。補完的統制とは、他の統制の弱点や欠陥に関連するリスクを軽減または排除するために実施される代替的または追加の統制です。被監査企業が技術的、運用上、財務上、またはその他の制約により当初の監査勧告を実施できない場合、かつ補完的統制が同等またはそれと同等のレベルの保証を提供できる場合には、未解決の問題に対する補完的統制の推奨が適切となる可能性があります。ただし、未解決の問題に対する補完的統制の推奨には、未解決の問題に起因する残存リスクの事前評価が必要であり、これは補完的統制が必要かつ実現可能かどうかを判断する上でより重要です。

参考文献：

- * フォローアップ監査 - カナダ監査 説明責任財団 1
- * 監査フォローアップの実施：検証のタイミング - 監査人 2
- * 内部監査のフォローアップ：本当に労力に見合う価値があるのか？

最新問題: 901

_____は、可能な限り早い段階でデータの整合性を確保するために、データ準備の段階で実装されるべきである。

- A. 管理合計
- B. 認証制御
- C. パリティビット
- D. 認証制御

Answer: A ([メッセージを残す](#))

セクション：情報資産の保護

説明

Explanation:

データ整合性を可能な限り早い段階で確保するため、管理合計はデータ準備の段階から導入すべきである。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 902

A database administrator is responsible for:

- A. defining data ownership.
- B. establishing operational standards for the data dictionary.
- C. creating the logical and physical database.
- D. establishing ground rules for ensuring data integrity and security.

Answer: (解答を表示する)

Explanation/Reference:

Explanation:

A database administrator is responsible for creating and controlling the logical and physical database.

Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

最新問題: 903

When conducting a requirements analysis for a project, the BEST approach would be to:

- A. prototype the requirements,
- B. consult key stakeholders
- C. test operational deliverable
- D. conduct a control self-assessment

Answer: A (メッセージを残す)

最新問題: 904

管理自己評価を実施する際に、時間とコストの面で最も効率的な方法はどれでしょうか？

(CSA)は、広範囲に分散した多数の従業員を抱える組織にとってどのようなものなのでしょうか？

- A. トップダウン分析とボトムアップ分析
- B. 対面インタビュー
- C. アンケート調査票
- D. ファシリテーター付きワークショップ

Answer: C (メッセージを残す)

セクション :ITのガバナンスと管理

最新問題: 905

次のソフトウェア開発手法のうち、疎結合された独立したコンポーネントを定義、実装、構成してシステムに組み込むための再利用ベースのアプローチはどれですか？

- A. アジャイル開発

B. ソフトウェアプロトタイピング

C. 迅速なアプリケーション開発

D. コンポーネントベース開発

Answer: ([解答を表示する](#))

説明／参考資料：

コンポーネントベースソフトウェアエンジニアリング (CBSE) (コンポーネントベース開発 (CBD)とも呼ばれる)は、ソフトウェアシステム全体にわたる幅広い機能に関して、関心の分離を重視するソフトウェアエンジニアリングの一分野です。これは、疎結合された独立したコンポーネントを定義、実装、構成してシステムに組み込むための再利用ベースのアプローチです。この手法は、ソフトウェア自体と、そのようなソフトウェアを支援する組織の両方にとって、短期的にも長期的にも、同様に幅広いメリットをもたらすことを目指しています。

ソフトウェアエンジニア (誰? は、コンポーネントをサービス指向の出発点となるプラットフォームの一部とみなしている。コンポーネントは、例えばWebサービスにおいて、そして近年ではサービス指向アーキテクチャ (SOA)において、このような役割を果たします。SOAでは、コンポーネントはWebサービスによってサービスに変換され、その後、通常のコンポーネントの特性を超えたさらなる特性を継承します。

コンポーネントはイベントを生成または消費することができ、イベント駆動型アーキテクチャ (EDA)に使用できます。

構成要素の定義と特性

個々のソフトウェアコンポーネントとは、関連する一連の機能 (またはデータ)をカプセル化したソフトウェアパッケージ、Webサービス、Webリソース、またはモジュールのことです。

すべてのシステムプロセスは個別のコンポーネントに配置され、各コンポーネント内のすべてのデータと関数は意味的に関連付けられています (クラスの内容と同様)。この原則により、コンポーネントはモジュール化され、凝集性が高いとよく言われます。システム全体の連携に関して、コンポーネントはインターフェースを介して相互に通信します。コンポーネントがシステムの他の部分にサービスを提供する場合、他のコンポーネントが利用できるサービスとその利用方法を指定する提供インターフェースを採用します。このインターフェースはコンポーネントの署名と見なすことができ、クライアントはコンポーネントを利用するために内部動作 (実装を知る必要はありません。この原則により、コンポーネントはカプセル化されていると呼ばれます。この記事のUML図では、提供インターフェースはコンポーネントの外縁に付いたロリポップ記号で表されています。

しかし、コンポーネントが機能するために別のコンポーネントを使用する必要がある場合、そのコンポーネントは必要なサービスを指定する使用インターフェースを採用します。この記事のUML図では、使用インターフェースはコンポーネントの外縁に付された開いたソケットシンボルで表されます。

仮想的な休暇予約システムをUML 2.0で表現した、複数のソフトウェアコンポーネントの簡単な例を示します。

コンポーネントのもう一つの重要な特性は、代替可能であることです。つまり、後継コンポーネントが元のコンポーネントの要件 (インターフェースを介して表現される)を満たしていれば、設計時または実行時に、あるコンポーネントを別のコンポーネントに置き換えることができます。その結果、コンポーネントは、そのコンポーネントが動作するシステムを壊すことなく、更新版または代替品に置き換えることができます。

部品を交換する際の一般的な目安として、部品Bが部品Aと同等以上の機能を提供し、かつ部品Aが使用していた量を超えない場合、部品Bは部品Aを直ちに置き換えることができる。

ソフトウェアコンポーネントは、多くの場合、オブジェクト (クラスではなく)またはオブジェクトの集合 (オブジェクト指向プログラミングによる)の形で、バイナリ形式またはテキスト形式で表現され、何らかのインターフェース記述言語 (IDL)に準拠しているため、コンピュータ内の他のコンポーネントから独立して存在することができる。

コンポーネントを複数の実行コンテキストやネットワークリンク間でアクセスまたは共有する場合、コンポーネントを宛先に届けるために、シリアルライゼーションやマーシャリングなどの技術がよく用いられます。

再利用性は、高品質なソフトウェアコンポーネントの重要な特性です。プログラマーは、多くの異なるプログラムで再利用できるようにソフトウェアコンポーネントを設計・実装する必要があります。

さらに、ソフトウェアコンポーネントがユーザーと直接やり取りする場合は、コンポーネントベースのユーザビリティテストを検討すべきである。

効果的に再利用できるソフトウェアコンポーネントを作成するには、相当な努力と意識が必要です。コンポーネントは以下の条件を満たす必要があります。

完全に文書化されています

徹底的にテスト済み

堅牢性 - 包括的な入力妥当性チェック機能付き

適切なエラーメッセージまたはリターンコードを返すことができる

予期せぬ用途に使用されることを念頭に置いて設計されている

以下の回答は誤りでした。

アジャイル開発 - アジャイルソフトウェア開発とは、反復的かつ漸進的な開発に基づいたソフトウェア開発手法のグループであり、自己組織化された異分野横断型チーム間のコラボレーションを通じて要件とソリューションが進化していくものです。

ソフトウェアプロトタイピングとは、ソフトウェアアプリケーションのプロトタイプ、つまり開発中のソフトウェアプログラムの不完全なバージョンを作成する活動を指します。これはソフトウェア開発において行われる活動であり、機械工学や製造業など他の分野で知られているプロトタイピングに匹敵するものです。

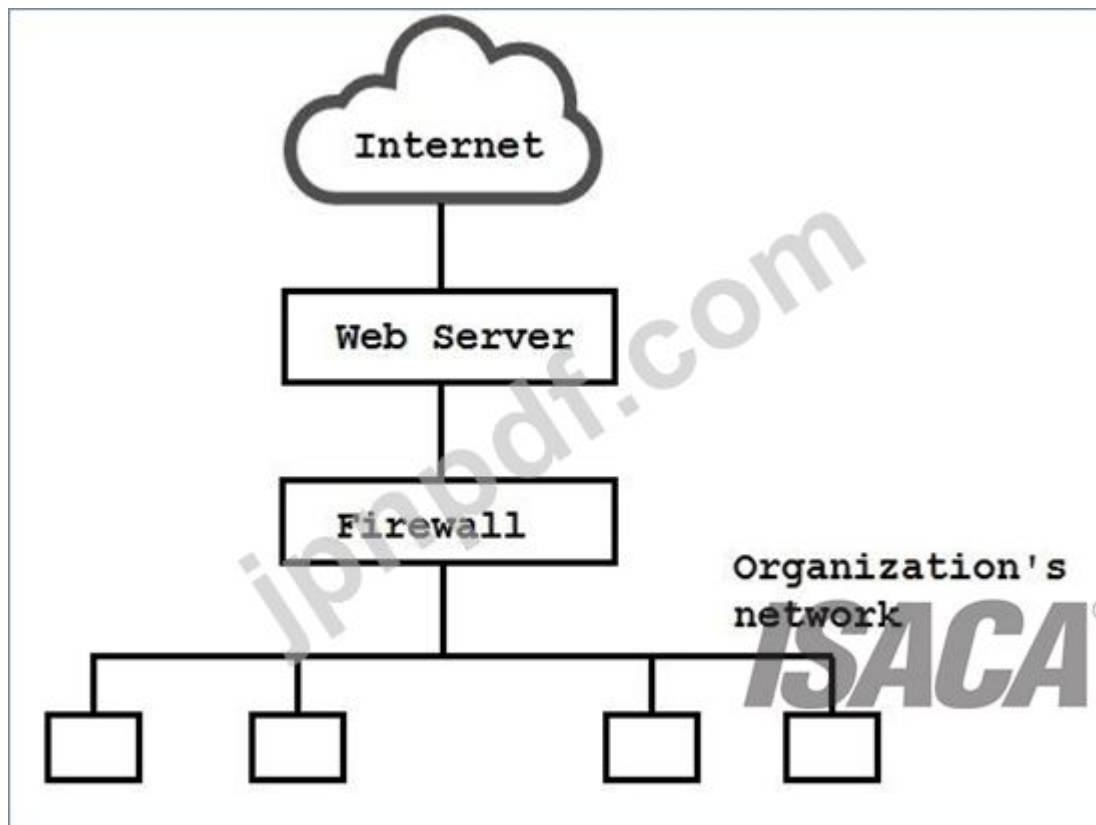
ラピッドアプリケーション開発 (RAD) は、計画を最小限に抑え、迅速なプロトタイピングを重視するソフトウェア開発手法です。RADを用いたソフトウェア開発では、計画はソフトウェア開発そのものと並行して行われます。綿密な事前計画が不要なため、一般的にソフトウェア開発速度が大幅に向上し、要件変更も容易になります。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 194ページ

最新問題: 906

ファイアウォールが認識できない攻撃の試みを検出するために、IS監査担当者は、ネットワーク侵入検知システム (IDS) を以下の場所に設置することを推奨すべきです。



- A. ファイアウォールと組織のネットワーク。
- B. インターネットとファイアウォール。
- C. インターネットとウェブサーバー。
- D. Webサーバーとファイアウォール。

Answer: A ([メッセージを残す](#))

説明／参考資料：

Explanation:

ファイアウォールと組織のネットワークの間にネットワークベースの侵入検知システムを配置すれば、ファイアウォールで認識できない攻撃試行も検知できます。インターネットとファイアウォールの間にネットワークベースの侵入検知システムを配置すれば、攻撃試行がファイアウォールを通過するかどうかにかかわらず、攻撃試行を検知できます。

最新問題: 907

以下のメッセージサービスのうち、特定のアクションが発生したことを示す最も強力な証拠となるのはどれですか？

- A. 配達証明
- B. 否認禁止
- C. 提出証明
- D. メッセージ発信元認証

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

否認防止サービスは、特定のアクションが発生したことの証拠を提供します。否認防止サービスは、送信証明、配信証明、メッセージ発信元認証といった、より弱い証明手段と類似しています。しかし、否認防止は、第三者に対して証明を提示できるため、

より強力な証拠となります。否認防止にはデジタル署名が使用されます。メッセージ発信元認証は、メッセージの発信元を確認するだけで、完了した仕様を確認するものではありません。

最新問題: 908

Upon completion of audit work, an IS auditor should:

- A. provide a report to senior management prior to discussion with the auditee.
- B. distribute a summary of general findings to the members of the auditing team.
- C. provide a report to the auditee stating the initial findings.
- D. review the working papers with the auditee.

Answer: ([解答を表示する](#))

Explanation

Upon completion of audit work, an IS auditor should distribute a summary of general findings to the members of the auditing team. This is to ensure that the audit team members are aware of the audit results, have an opportunity to provide feedback, and can agree on the audit conclusions and recommendations. Providing a report to senior management prior to discussion with the auditee, providing a report to the auditee stating the initial findings, and reviewing the working papers with the auditee are not appropriate actions for an IS auditor to take upon completion of audit work, as they may compromise the audit independence, objectivity, and quality. References: ISACA CISA Review Manual 27th Edition, page 221

最新問題: 909

次のネットワークサービスのうち、ドメイン名をネットワークIPアドレスまたはネットワークIPにマッピングするのはどれですか？

ドメイン名へのアドレス？

- A. DHCP
- B. DNS
- C. ディレクトリサービス
- D. ネットワーク管理

Answer: ([解答を表示する](#))

セクション：情報システムの運用、保守およびサポート

説明／参考資料：

ドメインネームシステム (DNS) - ネットワークノードの名前をネットワークIPアドレスに変換する。

試験に向けて、ネットワークサービスに関する以下の情報を知っておく必要があります。

コンピュータネットワークでは、ネットワークサービスとは、ネットワークアプリケーション層で実行されるアプリケーションであり、

上記のように、データの保存、操作、表示、通信、またはその他の機能を提供するものは、アプリケーション層ネットワークに基づくクライアント/サーバーまたはピアツーピアアーキテクチャを使用して実装されることが多い。

プロトコル。

各サービスは通常、1 台以上のコンピュータ (多くの場合、

専用サーバーコンピュータ (複数のサービスを提供) であり、ネットワーク経由でクライアントコンポーネントからアクセスされる。

他のデバイス上で実行できます。ただし、クライアントとサーバーのコンポーネントは両方とも同じデバイス上で実行できます。機械。

クライアントとサーバーには、多くの場合ユーザーインターフェースがあり、場合によってはそれらに関連するその他のハードウェアも備わっている。

ネットワークサービスの種類は以下のとおりです。

ネットワークファイルシステム - ネットワークファイルシステム (NFS) は、もともと開発された分散ファイルシステムプロトコルです。

1984年にSun Microsystemsによって開発され、クライアントコンピュータのユーザーがネットワーク経由でファイルにアクセスできるようにした。

ローカルストレージにアクセスします。

リモート アクセス サービス - リモート アクセス サービス (RAS) は、ハードウェアと

IT機器のネットワーク上に存在するツールや情報にリモートアクセスを可能にするソフトウェア。

ディレクトリサービス - ディレクトリサービスとは、情報を保存、整理し、アクセスを提供するソフトウェアシステムのことで

す。ディレクトリ内の情報。ソフトウェアエンジニアリングでは、ディレクトリは名前と値のマップです。

辞書のように、名前を指定して値を検索できます。辞書の単語には、

ディレクトリ内では、1つの名前が複数の異なる情報に関連付けられる場合があります、これは複数の定義が存在することを意味します。

同様に、単語には異なる品詞や異なる定義があるように、ディレクトリ内の名前には

さまざまな種類のデータがあります。

ネットワーク管理 - コンピュータ ネットワークでは、ネットワーク管理とは、活動、方法、運用、管理、保守、および提供に関連する手順とツール

ネットワークシステム。ネットワーク管理は指揮統制の実践に不可欠であり、一般的に

ネットワークオペレーションセンターから実行される。

動的ホスト構成プロトコル (DHCP) - 動的ホスト構成プロトコル (DHCP) は、

インターネットプロトコル (IP) ネットワークで動的に分散されるために使用される標準化されたネットワークプロトコル

ネットワーク構成パラメータ、インターフェースやサービスの IP アドレスなど。DHCP では、

コンピュータはDHCPサーバーからIPアドレスとネットワークパラメータを自動的に要求し、

ネットワーク管理者またはユーザーがこれらの設定を手動で構成する必要性。

電子メールサービス - 通信ネットワークに接続された端末またはPCを介して、

信頼できるメッセージを他の個人またはグループに送信する。

印刷サービス - 通常はネットワーク上のプリントサーバーを介して、印刷の管理と実行を行う機能を提供します。

ネットワーク上の他のデバイスからの印刷要求サービス

ドメインネームシステム (DNS) - ネットワークノードの名前をネットワークIPアドレスに変換する。

以下の回答は誤りでした。

動的ホスト構成プロトコル (DHCP) - 動的ホスト構成プロトコル (DHCP) は、

インターネットプロトコル (IP) ネットワークで動的に分散されるために使用される標準化されたネットワークプロトコル

ネットワーク構成パラメータ、インターフェースやサービスの IP アドレスなど。DHCP では、

コンピュータはDHCPサーバーからIPアドレスとネットワークパラメータを自動的に要求し、

ネットワーク管理者またはユーザーがこれらの設定を手動で構成する必要性。

ディレクトリサービス - ディレクトリサービスとは、情報を保存、整理し、アクセスを提供するソフトウェアシステムのことで

す。
ディレクトリ内の情報。ソフトウェアエンジニアリングでは、ディレクトリは名前と値のマップです。

辞書のように、名前を指定して値を検索できます。辞書の単語には、

ディレクトリ内では、1つの名前が複数の異なる情報に関連付けられる場合があります、これは複数の定義が存在することを意味しま

す。
同様に、単語には異なる品詞や異なる定義があるように、ディレクトリ内の名前には
さまざまな種類のデータがあります。

ネットワーク管理 - コンピュータ ネットワークでは、ネットワーク管理とは、活動、方法、
運用、管理、保守、および提供に関連する手順とツール

ネットワークシステム。ネットワーク管理は指揮統制の実践に不可欠であり、一般的に
ネットワークオペレーションセンターから実行される。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版 258ページ

最新問題: 910

侵入テストサイクルのどの段階で、テスターは特定された脆弱性を利用してターゲットシステムへのアクセスを試みますか？

- A. 漏出
- B. 搾取
- C. 偵察
- D. スキャン

Answer: B (メッセージを残す)

エクスプロイトとは、テスターが特定された脆弱性を利用して、システムへの不正アクセスを取得する段階のことです。

搾取（正解 B）

攻撃者は、SQLインジェクション、バッファオーバーフロー、権限昇格などの手法を用いる。

例 :テスターが脆弱なパスワードを悪用して管理者権限を取得する。

漏出（不正解 A）

アクセス権を取得した後、データを盗み出すプロセス。

偵察（不正解 C）

攻撃者が標的に関する情報を収集する初期段階。

スキャン（不正解 D）

開いているポートやサービスを特定する作業を含みますが、実際の攻撃は伴いません。

参考文献：

ISACA CISAレビューマニュアル

NIST 800-115 セキュリティテストに関する技術ガイド)

最新問題: 911

Which of the following would be the MOST useful metric for management to consider when reviewing a project portfolio?

- A. Net present value (NPV) of the portfolio

- B. Total cost of each project
- C. Expected return divided by total project cost
- D. Cost of projects divided by total IT cost

Answer: A ([メッセージを残す](#))

最新問題: 912

What is the PRIMARY purpose of documenting audit objectives when preparing for an engagement?

- A. To identify areas with relatively high probability of material problems
- B. To help prioritize and schedule auditee meetings
- C. To address the overall risk associated with the activity under review
- D. To help ensure maximum use of audit resources during the engagement

Answer: B ([メッセージを残す](#))

最新問題: 913

IS監査担当者が、あるベンダーが倒産しており、エスクロー口座に古いバージョンのソースコードが保管されていることを発見しました。監査担当者が組織に対して行うべき最善の推奨事項は何でしょうか？

- A. 現在の規制を覆す新しいアプリケーションを分析する
- B. ビジネスリスクを判断するための分析を実施する
- C. エスクローのバージョンを最新の状態に更新してください。
- D. 既存のコードを使用してアプリケーションをサポートするための保守計画を作成する

Answer: ([解答を表示する](#)**)**

つまり、組織はエスクローエージェントからソースコードを入手し、現在使用しているアプリケーションのバージョンと比較する必要があります。そして、エスクロー版に不足している、または異なる変更や更新を特定し、適用して、現在のバージョンと一致させる必要があります。

こうすることで、組織は現在のニーズと要件を反映した、完全かつ正確なソースコードのコピーを確実に取得できる。

エスクローのバージョンを最新の状態にすることで、組織は、古いバージョンや互換性のないバージョンのソースコードを使用することに伴うリスクやコストを回避または軽減できます。たとえば、古いバージョンのソースコードには、アプリケーションの機能、セキュリティ、またはパフォーマンスに影響を与える可能性のあるバグ、エラー、または脆弱性が含まれている場合があります。また、古いバージョンのソースコードには、アプリケーションの使いやすさ、効率性、または価値を向上させる可能性のある機能、拡張機能、または統合が欠けている場合もあります。さらに、古いバージョンのソースコードは、アプリケーションの品質、信頼性、または合法性に影響を与える可能性のある一部の標準、規制、または契約に準拠していない場合もあります¹。

他の選択肢は、組織にとってエスクローのバージョンを最新の状態にするほど良いものではありません。オプションA、現在の要件を満たす新しいアプリケーションを分析することは可能な選択肢ですが、既存のアプリケーションを更新するよりも時間とコストがかかり、リスクも高くなる可能性があります。組織は、新しいアプリケーションの選択、取得、実装、テスト、移行という複雑で長いプロセスを経る必要があります、業務やパフォーマンスに支障をきたす可能性があります。また、新しいアプリケーションに切り替える際に、互換性、相互運用性、データ品質の問題に対処する必要性が生じる可能性もあります²。オプションB、ビジネスリスクを判断するための分析を行うことは必要なステップですが、組織への推奨事項ではありません。組織は、ベンダーが倒産し、エスクローに古いバージョンのソースコードが含まれているアプリケーションを使用することによるビジネスリスクを既に認識しているはずです。組織は、このリスクを軽減または排除するためのソリューションを見つけて実装することに注力する必要があります³。オプションD、既存のコードを使用してアプリケーションをサポートするための保守計画を策定することは、組織が

既存のコードにアクセスできることを前提としているため、実行可能な選択肢ではありません。しかし、実際にはそうではありません。ベンダーは既に廃業しており、エスクローには古いバージョンのソースコードしか保管されていないからです。組織は、ソースコードの完全かつ正確なコピーがなければ、アプリケーションのサポートや保守を行うことができません。

参考文献：

- * ソースコードエスクローの重要性 - ISACA1
- * ソースコードエスクロー2の目的と理由
- * エスクローにおけるソースコードのロック解除 2023：安全なソフトウェアのためのガイド3

最新問題: 914

ある組織が買収を計画しており、対象企業のITガバナンスフレームワークを評価するためにIS監査人を雇いました。フレームワークの有効性を判断する上で、次のうちどれが最も役立つでしょうか？

- A. 最近の第三者機関によるIS監査報告書
- B. 現在および過去の内部IS監査報告書
- C. 競合他社とのITパフォーマンスベンチマークレポート
- D. IT能力と成熟度に関する自己評価レポート

Answer: A ([メッセージを残す](#))

最新問題: 915

最高情報責任者 (CIO) が情報システム部門 (IS) に対し、組織のITプロセスとシステムに対する複数のセキュリティ対策の実装を依頼した。監査担当者は、以下の対応を取るべきである。

- A. 独立問題のため拒否
- B. 監査管理部門に利益相反について報告する。
- C. 適切な専門的注意を払って、業務および今後の監査を実施する。
- D. 実施管理部門から実施の承認を得る。

Answer: ([解答を表示する](#)**)**

最新問題: 916

A requirement for biometric access to physical facilities is an example of which type of control?

- A. Corrective
- B. Preventive
- C. Detective
- D. Deterrent

Answer: ([解答を表示する](#)**)**

Biometric access control is a preventive control because it restricts physical entry to authorized individuals only, thereby preventing unauthorized access before it can occur.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題

集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (156230%OFF問題集溶と正解付き
で 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 917

An IS auditor reviewing the physical access section of a security plan for a data center should expect to find that:

- A. the data center has mantraps on entrances and exits.
- B. access to environmental controls is well labeled.
- C. the access devices are connected to a remote management system.
- D. entry points requiring different rules of access have been identified.

Answer: (解答を表示する)

最新問題: 918

デジタル署名の特徴は、以下の点です。

- A. データが変更されたときに検証されます。
- B. メッセージに固有のもの
- C. 受信機の制御下にある。
- D. 再現可能なハッシュアルゴリズムを備えている

Answer: B (メッセージを残す)

最新問題: 919

IS監査中に、組織の仮想サーバーファーム全体でセキュリティ構成が異なっていることが判明しました。IS監査担当者が統制環境を改善するために推奨する最善策は次のうちどれですか？

- A. 各サーバーのセキュリティ構成について独立したレビューを実施する
- B. 仮想サーバーのセキュリティ構成ベースラインを実装する
- C. 高リスク仮想サーバーに対するセキュリティ監視制御を実装する
- D. 仮想サーバーファーム全体で標準的なパッチ管理レビューを実施する

Answer: B (メッセージを残す)

セクション：情報システムの監査プロセス

最新問題: 920

データセンターにはバッジによる入退室システムがあります。センター内のコンピューティング資産を保護するために最も重要なのは次のうちどれですか？

- A. バッジリーダーは、不正操作が発覚しやすい場所に設置されています。
- B. バッジシステムを制御するコンピュータは頻繁にバックアップされます
- C. 紛失または盗難されたバッジを速やかに無効化する手続きが存在します
- D. バッジ入力の試みはすべて記録されます

Answer: (解答を表示する)

説明／参考資料：

Explanation:

バッジリーダーを不正操作してもドアは開かないため、これは無関係です。入退室試行のログ記録は、限定的な価値しかない可能性があります。最大の脅威は、従業員であるか否かを問わず、データセンターに侵入できる権限のない人物です。したがって、紛失または盗難されたバッジを無効化するプロセスが重要です。システムの構成は頻繁に変更されないため、頻繁なバックアップは必要ありません。

最新問題: 921

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

- A. digitally signing all e-mail messages.
- B. encrypting all e-mail messages.
- C. compressing all e-mail messages.
- D. password protecting all e-mail messages.

Answer: A ([メッセージを残す](#))

By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able to open the message; however, it would not ensure the authenticity of the sender.

最新問題: 922

Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?

- A. Evaluate configuration settings for the date of birth field requirements.
- B. Review new account applications submitted in the past month for invalid dates of birth
- C. Attempt to submit new account applications with invalid dates of birth
- D. Review the business requirements document for date of birth field requirements.

Answer: C ([メッセージを残す](#))

最新問題: 923

The auditor's final opinion is to be based on:

- A. The objectives and verbal statements made by management
- B. An understanding of management's desired audit results
- C. The audit committee's specifications
- D. The results of evidence and testing

Answer: D ([メッセージを残す](#))

The auditor is to be a professional skeptic who tests assertions of management and renders an opinion based on the evidence discovered during the audit.

最新問題: 924

情報セキュリティガバナンス委員会の主な責任は次のうちどれですか？

- A. 情報セキュリティ技術の購入を承認する
- B. 情報セキュリティ意識向上トレーニング戦略の承認

- C. 情報セキュリティ戦略の見直し
- D. 情報セキュリティポリシー遵守状況レビューの分析

Answer: C ([メッセージを残す](#))

セクション :ITのガバナンスと管理

最新問題: 925

組織の情報セキュリティポリシーが適切かどうかを判断する際に、情報セキュリティ監査担当者が使用する情報源として最適なものは、次のうちどれですか？

- A. リスク評価結果
- B. 貫通試験結果
- C. 業界ベンチマーク
- D. 情報セキュリティプログラム計画

Answer: ([解答を表示する](#)**)**

最新問題: 926

An IS auditor follows up on a recent security incident and finds the incident response was not adequate.

Which of the following findings should be considered MOST critical?

- A. The security weakness facilitating the attack was not identified.
- B. The attack was not automatically blocked by the intrusion detection system (IDS).
- C. The attack could not be traced back to the originating person.
- D. Appropriate response documentation was not maintained.

Answer: A ([メッセージを残す](#))

最近のセキュリティインシデントを調査するIS監査担当者にとって最も重要な発見は、攻撃を助長したセキュリティ上の弱点が特定されていないことです。これは、インシデントの根本原因が分析されておらず、攻撃の成功を許した脆弱性が修復されていないことを示しています。つまり、組織は今後も同様の攻撃にさらされる可能性があり、セキュリティ体制は改善されていないということです。セキュリティ上の弱点を特定し、対処することは、インシデント対応プロセスにおける重要なステップであり、再発防止、影響の軽減、回復力の向上に役立ちます。

その他の調査結果は、セキュリティ上の弱点を特定できなかったことほど重大なものではありませんが、組織が対処すべき重要な問題です。侵入検知システム (IDS)によって攻撃が自動的にブロックされなかったという調査結果は、IDSが適切に構成されていなかったか、攻撃を検出および防止するための最新のシグネチャやルールがなかったことを示唆しています。攻撃の発信元を特定できなかったという調査結果は、組織が攻撃者を特定して帰属させるための十分なログ記録、監視、またはフォレンジック機能を備えていなかったことを示唆しています。適切な対応文書が維持されていなかったという調査結果は、組織が一貫した正式なインシデント対応手順に従っていなかったか、インシデントから得られた行動、決定、および教訓を文書化していなかったことを示しています。

参考文献：

- * ISACA CISAレビューマニュアル第27版 (2019年)、254ページ
- * インシデント対応プロセス - ISACA1
- * インシデント対応 :セキュリティ上の脆弱性を特定し、修正する方法

最新問題: 927

以下のオンライン監査手法のうち、エラーや不正を早期に発見するのに最も効果的なものはどれですか？

- A. 組み込み監査モジュール
- B. 総合試験施設
- C. スナップショット
- D. 監査フック

Answer: D ([メッセージを残す](#))

監査フック技術とは、特定のトランザクションを検査するために、アプリケーションシステムにコードを埋め込む手法です。これにより、情報システム監査担当者は、エラーや不正が深刻化する前に対応することができます。組み込み監査モジュールとは、組織のホストアプリケーションシステムに特別に作成されたソフトウェアを組み込み、アプリケーションシステムを選択的に監視する手法です。テストデータの使用が現実的でない場合は統合テスト機能が使用され、監査証跡が必要な場合はスナップショットが使用されます。

最新問題: 928

重要なレガシーシステムを新しいシステムに移行する際に、以下のうちどれが最大の危険をもたらすでしょうか？
システム？

- A. アジャイル開発手法を採用
- B. 段階的なアプローチに従う
- C. 直接切り替え方式を採用
- D. 並列システムの維持

Answer: C ([メッセージを残す](#))

セクション：情報システムの取得、開発、導入

最新問題: 929

Which of the following presents the GREATEST concern when implementing data flow across borders?

- A. Political unrest
- B. Equipment incompatibilities
- C. Software piracy laws
- D. National privacy laws

Answer: ([解答を表示する](#))

最新問題: 930

ITガバナンス機関は、ITサービスの提供が一貫して効果的なプロセスに基づいているかどうかを判断したいと考えています。次のうち、最適なアプローチはどれですか？

- A. 成熟度モデルを開発する。
- B. コントロール自己評価 (CSA) を実施する。
- C. ギャップ分析を実施する。
- D. 主要業績指標 (KPI) を評価する。

Answer: D ([メッセージを残す](#))

最新問題: 931

次のうち、ネットワーク情報を監視および記録するネットワーク診断ツールはどれですか？

- A. オンラインモニター
- B. ダウンタイムレポート
- C. ヘルプデスクレポート
- D. プロトコルアナライザー

Answer: ([解答を表示する](#))

説明／参考資料：

Explanation:

プロトコルアナライザは、ネットワーク診断ツールであり、アナライザが接続されているリンクを流れるパケットからネットワーク情報を監視および記録します。オンラインモニタ（選択肢）は、電気通信伝送を測定し、伝送が正確かつ完全であったかどうかを判断します。

ダウンタイムレポート（選択肢）は、通信回線および回路の可用性を追跡します。ヘルプデスクレポート（選択肢）は、ヘルプデスクによって作成されます。ヘルプデスクは、情報システム運用中に発生する問題に対処するための訓練を受けた情報システム技術サポート担当者によって運営またはサポートされています。

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **932**

仮想化環境において最も重要な制御は次のうちどれですか？

- A. 仮想化環境の運用に関するポリシーの定期的な更新
- B. ハイパーバイザーとゲストマシンのセキュリティ強化
- C. ハードウェアリソースとネットワークコンポーネントの冗長性
- D. ゲストオペレーティングシステムレベルでのリソース利用状況の監視

Answer: B ([メッセージを残す](#))

説明

仮想化環境において最も重要な対策は、ハイパーバイザーとゲストマシンのセキュリティ強化である。

ハードニングとは、システムやデバイスの脆弱性やリスクを軽減するために、セキュリティ対策や構成を適用するプロセスです。ハイパーバイザとゲストマシンのハードニングは、仮想化環境を攻撃から保護するために不可欠です。なぜなら、これらの環境は物理層と仮想層の両方から様々な脅威にさらされているからです。ハイパーバイザとゲストマシンのハードニングには、以下の手順が含まれます。

ハイパーバイザーとゲストオペレーティングシステム、およびそれら上で動作するアプリケーションとドライバに対して、最新のパッチとアップデートを適用する。

ハイパーバイザーとゲストマシンのファイアウォールとネットワーク設定を構成し、ネットワークトラフィックを制限および監視し、不正アクセスや不正通信を防止します。

ハイパーバイザーおよびゲストマシン上の不要な機能、サービス、アカウント、ポートを無効化または削除することで、攻撃対象領域を最小限に抑え、攻撃者による侵入経路の可能性を低減します。

ハイパーバイザーとゲストマシンに対して強力な認証および認可ポリシーを適用し、認可されたユーザーまたは管理者のみがアクセスまたは管理できるようにします。

ハイパーバイザーおよびゲストマシンのデータと通信を暗号化することで、それらに保存または送信される情報の機密性と完全性を保護します。

ハイパーバイザーとゲストマシンに対してログ記録および監査メカニズムを実装し、それら上で発生するあらゆる活動やイベントを記録および追跡し、あらゆるインシデントや異常を検出および調査できるようにする。

ハイパーバイザーとゲストマシンのセキュリティ強化は、仮想化環境に対する一般的な攻撃（例：[Denial of Service](#)）を防止または軽減するのに役立ちます。

ハイパーバイザーからの脱出：悪意のあるゲストマシンが隔離された環境から脱出し、ハイパーバイザーまたは他のゲストマシンへのアクセス権を取得する攻撃。

ハイパーバイザー侵害：攻撃者がハイパーバイザーの脆弱性や設定ミスが悪用して、ハイパーバイザーまたはそのリソースを制御下に置く攻撃。

ゲスト侵害：攻撃者がゲストマシンの脆弱性や設定ミスが悪用して、そのデータやアプリケーションにアクセスする攻撃。

ゲストなりすまし：攻撃者が偽のゲストマシンまたはクローンを作成し、他のゲストやユーザーを騙してそのマシンとやり取りさせる攻撃。

ゲストサービス拒否攻撃：攻撃者がゲストマシンのリソースを消費または枯渇させることで、その可用性やパフォーマンスを阻害する攻撃。

したがって、ハイパーバイザーとゲストマシンのセキュリティ強化は、仮想化環境のセキュリティ、信頼性、パフォーマンスを向上させる上で最も重要な対策です。仮想化環境のセキュリティ強化に関する詳細については、以下のWebサイトを参照してください。

Azure フリートにおけるハイパーバイザーのセキュリティ

第2章 Hyper-Vホストのセキュリティ強化

Windows Server における Hyper-V セキュリティの計画

最新問題: 933

SSLネットワークプロトコルはどのようにして機密性を確保するのですか？

- A. RSAなどの対称暗号化によって
- B. データ暗号化標準 (DES)などの非対称暗号化方式による
- C. Advanced Encryption Standard (AES)などの非対称暗号化方式による
- D. データ暗号化標準 (DES)などの対称暗号化方式による

Answer: D ([メッセージを残す](#))

説明／参考資料：

Explanation:

SSLプロトコルは、データ暗号化などの対称暗号化によって機密性を提供します。

標準規格、またはDES。

最新問題: 934

ネットワークの脆弱性に関する外部評価において、最も重要な検証事項は何ですか？

- A. セキュリティ情報イベント管理 (SIEM) ルールの更新
- B. ネットワークセキュリティポリシーの定期的な見直し
- C. ネットワーク資産インベントリの完全性
- D. 侵入検知システム (IDS) の設置場所

Answer: ([解答を表示する](#))

ネットワーク脆弱性の外部評価とは、外部の視点からネットワークのセキュリティと可用性に影響を与える弱点やリスクを特定し、評価するプロセスです。このプロセスにおいて最も重要な検証事項は、ネットワーク資産インベントリの完全性です。ネットワーク資産インベントリとは、ネットワークに接続されている、またはネットワークの一部となっているすべてのデバイス、システム、ソフトウェアのリストです。完全かつ正確なネットワーク資産インベントリがあれば、ネットワークの範囲と境界、潜在的な攻撃経路と侵入経路、重要な資産と依存関係、既存のセキュリティ制御とギャップを特定するのに役立ちます。ネットワーク資産インベントリが完全でない場合、ネットワーク脆弱性の外部評価では重要な資産や脆弱性が見落とされ、結果や推奨事項が不正確または不完全になる可能性があります。

参考文献：

- * 1では、外部脆弱性スキャンとは何か、そしてネットワーク資産の完全なインベントリを持つことがなぜ重要なのかを説明します。
- * 2では、ネットワークの脆弱性評価を包括的に実施する方法に関するガイドを提供し、ネットワーク資産を把握することの重要性を強調しています。
- * 3では、内部および外部の脆弱性スキャンを比較し、両方のタイプについて包括的なネットワーク資産インベントリが必要であることを強調しています。

最新問題: 935

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

- A. An increased number of people using technology
- B. Significant cost savings, through a reduction in the complexity of information technology
- C. A weaker organizational structures and less accountability
- D. Increased information protection (IP) risk will increase

Answer: ([解答を表示する](#))

BPRプロジェクトは、テクノロジーを利用する人の数の増加につながることが多く、これは懸念すべき点となる。不正解:

- B. BPRは技術指向であることが多く、この技術は従来よりも複雑で不安定なため、この分野ではコスト削減が実現することはあまりありません。
- D. プロジェクトが適切に実行されない限り、IP が BPR プロジェクトと競合する理由はありません。

最新問題: 936

監査担当者として、情報システムにおいて機密性、完全性、真正性、可用性が適切に実装されていることを確認することは非常に重要です。以下の定義のうち、これらのパラメータを誤って説明しているのはどれですか？

1. 真正性 - 第三者は、メッセージの内容が特定の主体によって送信されたものであり、他の誰によっても送信されたものではないことを検証できなければならない。
2. 否認防止— 特定のメッセージの発信元または受信元は、第三者によって検証可能でなければならない。メッセージの発信者が署名している場合、送信者はメッセージの送信を否認することはできない。
3. 説明責任 - 組織の行為は、異なる組織に明確に追跡可能でなければならない。

4. 可用性 - ITリソースは、任務の要件を満たすため、または重大な損失を回避するために、タイムリーに利用可能でなければなりません。

A. 提示されたすべての選択肢

B. 提示された選択肢のいずれにも該当しない

C. オプション1と2

D. 選択肢3

Answer: D (メッセージを残す)

セクション：情報資産の保護

Explanation:

質問を注意深く読むことが重要です。誤って」という言葉がキーワードでした。提示された定義のうち、どれが間違っているかを見つける必要がありました。アカウントビリティの定義は適切に説明されていませんでした。

以下に適切な定義を示します。

正しい定義は以下のとおりです。

真正性 - 第三者が、メッセージの内容が特定の組織からのものであり、他の組織からのものではないことを検証できなければならない。

否認防止 — 特定のメッセージの発信元または受信元は、第三者によって検証可能でなければならない。メッセージの発信者が署名している場合、送信者はメッセージの送信を否認することはできない。

説明責任 - 組織の行動は、その組織に明確に追跡可能でなければならない。ネットワークの可用性 - IT リソースは、任務の要件を満たすため、または重大な損失を回避するために、タイムリーに利用可能でなければならない。

参照：

CISAレビューマニュアル2014年版 34ページ

最新問題: 937

ITガバナンスレビューで得られた以下の所見のうち、最も懸念すべきものはどれですか？

A. IT予算は監視されていません

B. すべてのITサービスは第三者によって提供されます。

C. IT価値分析は完了していません。

D. ITは2種類の異なるオペレーティングシステムをサポートしています。

Answer: C (メッセージを残す)

IT価値分析が完了していないことは、ITガバナンスレビューにおいて最も懸念すべき所見です。IT価値分析とは、組織の目標と目的に対するITの貢献を測定し、実証するプロセスです。IS監査人は、IT価値分析の欠如を懸念すべきです。これは、IT投資とリソースがビジネスニーズと期待に合致していない、あるいはITのパフォーマンスと成果が監視・評価されていないことを示している可能性があるからです。その他の選択肢は、それほど重要ではない所見であり、ITガバナンスに大きな影響を与えない可能性があります。参考文献：

CISAレビューマニュアル (デジタル版)、第5章、セクション5.11

CISA復習問題、解答、解説データベース、問題ID 218

最新問題: 938

Which of the following BEST helps to ensure data integrity across system interfaces?

A. Access controls

- B. Environment segregation
- C. Reconciliations
- D. System backups

Answer: A ([メッセージを残す](#))

最新問題: 939

IS監査中にできるだけ多くの異常を検出するための最も効果的な方法はどれですか？

- A. プロセス全体について説明してください。
- B. 抽出した記録に対して実質的な検査を実施する。
- C. 主要プロセスの判断サンプリングを実施する。
- D. データ分析ツールを使用して傾向を特定する。

Answer: D ([メッセージを残す](#))

データ分析ツールは、情報システム監査において可能な限り多くの異常を検出する最も効果的な方法です。なぜなら、大量のデータを処理し、複雑な計算を実行し、パターン、外れ値、異常、または期待される結果からの逸脱を明らかにする視覚化を生成できるからです。データ分析ツールは、監査担当者がサンプルではなくデータ全体をテストし、継続的な監査と監視を実行するのにも役立ちます。

参考文献

ISACA CISAレビューマニュアル、第27版、256ページ

問題解決とは何か？手順、プロセス、テクニック | ASQ

監査人のためのデータ分析 - IIA

最新問題: 940

Which of the following is MOST important for an IS auditor to determine during the detailed design phase of a system development project?

- A. Program coding standards have been followed
- B. Acceptance test criteria have been developed
- C. Data conversion procedures have been established.
- D. The design has been approved by senior management.

Answer: B ([メッセージを残す](#))

The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase.

Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 323

最新問題: 941

IT運営委員会の主な責任は次のうちどれですか？

- A. IT戦略の統合に関する取り組みのレビューと支援
- B. ITセキュリティ戦略の策定と評価
- C. セキュリティとビジネス目標を統合するためのプロセスの実装
- D. セキュアなシステム開発フレームワークの開発と実装

Answer: A ([メッセージを残す](#))

これは、IT運営委員会が、IT戦略が組織の事業戦略、ビジョン、目標と整合し、それらを支援することを保証する責任を負っていることを意味します。IT運営委員会はまた、主要なITイニシアチブ、プロジェクト、投資を監督および承認し、それに応じてリソースと優先順位を割り当てる責任も負っています¹²。

ITセキュリティ戦略 B)の策定と評価は、IT運営委員会の主な責任ではなく、むしろIT戦略の特定の側面であり、小委員会または専任のセキュリティ機能に委任される可能性があります。IT運営委員会はITセキュリティ戦略に関するガイダンスと監督を提供することはできますが、その策定と評価に直接関与することはありません¹²。

セキュリティをビジネス目標と統合するプロセスを実装することは、IT運営委員会の主な責任ではなく、IT管理部門やスタッフが行う可能性のある運用上のタスクです。IT運営委員会はセキュリティプロセスの有効性を監視および評価することはできますが、その実装に直接関与することはありません¹²。

セキュアシステム開発フレームワーク D)の開発と実装は、IT運営委員会の主な責任ではなく、IT開発者やエンジニアが行う技術的な作業です。IT運営委員会はセキュアシステム開発フレームワークを承認および支持することはできますが、その開発と実装に直接関与することはありません¹²。

最新問題: **942**

Which of the following is the PRIMARY purpose of utilizing data analytics tools in audits?

- A. To speed up the audit process by reducing the need for documentation and testing
- B. To identify patterns in large data sets for more targeted audit procedures
- C. To provide assurance of the accuracy of financial data
- D. To increase the ease and use of automated audit processes

Answer: B ([メッセージを残す](#))

The primary purpose of using data analytics tools in audits is to analyze large volumes of data to detect patterns, trends, anomalies, or irregularities. This enables auditors to focus their testing and procedures on high-risk areas, thereby improving audit effectiveness and precision.

最新問題: **943**

問題解決の際に多数の変数を考慮できる能力を持つため、不正行為の検出に効果的なのは次のうちどれですか？

- A. エキスパートシステム
- B. ニューラルネットワーク
- C. 統合同期システム
- D. マルチタスクアプリケーション

Answer: B ([メッセージを残す](#))

説明／参考資料：

Explanation:

ニューラルネットワークは、問題を解決しようとする際に多数の変数を考慮できる能力を持っているため、不正行為の検出に効果的である。

最新問題: 944

During the audit of a database server, which of the following would be considered the GREATEST exposure?

- A. The password does not expire on the administrator account
- B. Default global security settings for the database remain unchanged
- C. Old data have not been purged
- D. Database activity is not fully logged

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

最新問題: 945

組織が外部顧客向けの技術サポートをアウトソーシングすることを決定した場合、IS監査担当者は以下のうちどれを主要な重点分野として推奨すべきでしょうか？

- A. 監査権が契約書に含まれていることを確認してください。
- B. 第三者との契約に関連するコストを最小限に抑える。
- C. 変更に対する顧客満足度をモニタリングする
- D. サービスレベル契約 (SLA) を現在のニーズに合わせる

Answer: ([解答を表示する](#)**)**

最新問題: 946

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- A. Dumping the memory content to a file
- B. Generating disk images of the compromised system
- C. Rebooting the system
- D. Removing the system from the network

Answer: C ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 947

An IS auditor is reviewing an organization's overall incident response capability following recovery from a cybersecurity incident. Which of the following findings should be of MOST concern to the auditor?

- A. Lessons learned were not documented after the incident.
- B. Logs were only collected as part of the post-incident review.
- C. Risk analysis errors were identified as part of the post-incident review.
- D. The incident was caused by a known vulnerability with a documented risk acceptance.

Answer: (解答を表示する)

最新問題: 948

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

- A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.
- B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
- C. Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
- D. Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Answer: A (メッセージを残す)

Explanation/Reference:

Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

最新問題: 949

侵入検知システム (IDS)には、多くの既知の弱点があります。次のうち、IDSの制限事項ではないものはどれですか？

- A. 識別および認証方式に脆弱性がある。
- B. アプリケーションレベルの脆弱性。
- C. アプリケーションへのバックドア
- D. ゼロデイ攻撃を検出します。

Answer: D (メッセージを残す)

説明／参考資料：

ゼロデイ攻撃の検出は、挙動検出やヒューリスティック検出を利用するIDSシステムの利点の一つです。

質問を注意深く読むことが重要です。NOT」という言葉が鍵でした。

侵入検知システムは適用範囲がやや限定されており、以下の点には対応していません。

政策定義の弱点

アプリケーションレベルの脆弱性

アプリケーション内のバックドア

識別および認証方式の脆弱性

また、CISA試験に向けて、以下の情報も知っておく必要があります。

IDSは、ルーターやファイアウォールと連携して、ネットワーク使用状況の異常を監視する。

IDSの広範なカテゴリには以下が含まれます。

1. ネットワークベースのIDS

2. ホストベースIDS

ネットワークベースのIDS

監視対象ネットワーク内での攻撃を特定し、オペレーターに警告を発する。

ネットワークベースのIDSをインターネットとファイアウォールの間に配置すれば、ファイアウォールを侵入するかどうかにかかわらず、すべての攻撃試行を検出できます。

ネットワークベースのIDSは、暗号化されたトラフィックを処理する際に機能不全に陥る。

ホストベースIDS

これらは特定の環境に合わせて設定されており、オペレーティングシステムのさまざまな内部リソースを監視して、潜在的な攻撃を警告します。

実行可能プログラムの変更を検知したり、ファイルの検出を検知したり、特権アカウントを使用しようとした際に警告を発したりすることができる。

これらは復号化されたトラフィックを監視することができ、ネットワークベースのIDSを補完する。

IDSの種類には以下が含まれます。

統計ベースのIDS - これらのシステムでは、システムの既知の動作と予想される動作を包括的に定義する必要があります。

ニューラルネットワーク - この機能を備えたIDSは、ネットワーク上のアクティビティとトラフィックの一般的なパターンを監視し、データベースを作成します。これは統計モデルに似ていますが、自己学習機能が追加されています。

シグネチャベースのIDS - これらのIDSシステムは、検出された侵入パターンから保護します。識別可能な侵入パターンは、シグネチャの形式で保存されます。

以下の回答は誤りでした。

挙げられたその他の選択肢はすべて、IDSの限界点である。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版、346ページと347ページ

最新問題: 950

IS監査担当者は、支払計算を扱うシステムへの変更に関するテスト結果を評価する。

監査人は、計算の 50% が事前に定められた合計と一致しないことを発見しました。

監査における次のステップとして最も可能性が高いのは次のうちどれでしょうか？

A. 誤りのある計算について、さらにテストを設計する。

B. 検査結果が不正確になった原因となりうる変数を特定する。

C. いくつかのテストケースを調べて結果を確認します。

D. 結果を文書化し、調査結果、結論、および提言をまとめた報告書を作成する。

Answer: C ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

IS監査担当者は次に、計算ミスが発生した事例を調査し、その結果を確認する必要がある。

計算結果が確認された後、さらなるテストを実施し、レビューすることができます。報告準備、調査結果、および提言は、すべての結果が確認されるまで行われません。

最新問題: 951

PDCAサイクルの以下のステップのうち、計画の実施、プロセスの実行、製品の製造を行うのはどれですか？

A. 計画

B.

C. チェック

D. 行動

Answer: B ([メッセージを残す](#))

セクション :ITのガバナンスと管理

説明／参考資料：

実行 - 計画を実行し、プロセスを実行し、製品を作成します。チャート作成と分析のためのデータを収集します。

以下の「確認」および「実行」の手順。

試験を受けるにあたっては、以下の情報を知っておく必要があります。

PDCA（計画・実行・評価・改善または計画・実行・評価・調整）は、

プロセスと製品の管理と継続的な改善のためのビジネス。

デミングサイクル、スチュワートサイクル、コントロールサイクル、または計画・実行・評価・改善（PDCA）サイクル。

このPDCAサイクルのバージョンはOPDCAです。追加された「O」は観察を意味します。

「現状を把握せよ。」

PDCAサイクルの各ステップは以下のとおりです。



プラン

期待される成果物に応じて結果を出すために必要な目標とプロセスを確立する

（目標または目的）。出力の期待値を設定することで、仕様の完全性と正確性は

これも目標とする改善策の一環です。可能であれば、小規模で開始して効果を検証してください。

する

計画を実行し、プロセスを実行し、製品を作成します。チャート作成と分析のためにデータを収集します。

「確認」と「実行」の手順に従う。

チェック

実際の結果（上記の DO」で測定・収集されたもの）を調べ、期待される結果と比較する。

（計画」からの目標または目的）の相違点を確認する。実施における逸脱を探す。

計画を確認し、実行を可能にするための計画の適切性と完全性も確認します。

実行」。データをグラフ化することで、複数のPDCAサイクルにわたる傾向を把握しやすくなり、収集したデータを情報に変換する。情報は次のステップ「行動」に必要なものだ。

活動

実際の結果と計画された結果の大きな差異について、是正措置を要求します。

違いを特定して根本原因を突き止める。変更を適用する場所を決定する。

プロセスまたは製品の改善。これら4つのステップを実行しても改善の必要性が生じない場合

改善するために、PDCA の適用範囲を、より詳細に計画および改善するように細分化することができます。

サイクルの次の反復、またはプロセスの別の段階に注意を向ける必要がある。

以下の回答は誤りです。

計画 - 目標とプロセスを確立し、

期待される成果（目標または目的）。

チェック - 実際の結果（上記の DO」で測定および収集されたもの）を調べ、

期待される結果（計画」からの目標または目的）との差異を確認する

ACT - 実際の結果と計画された結果の大きな違いについて是正措置を要求します。

違いを特定して根本原因を突き止める。変更を適用する場所を決定する。

プロセスまたは製品の改善

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版、107ページ

最新問題: 952

Which of the following BEST demonstrates that IT strategy is aligned with organizational goals and objectives?

A. IT strategies are communicated to all Business stakeholders

B. Organizational strategies are communicated to the chief information officer (CIO).

C. Business stakeholders are involved in approving the IT strategy.

D. The chief information officer (CIO) is involved in approving the organizational strategies

Answer: C ([メッセージを残す](#))

Business stakeholders being involved in approving the IT strategy best demonstrates that IT strategy is aligned with organizational goals and objectives. IT strategy is a plan that defines how IT resources and capabilities will support and enable the achievement of business goals and objectives. Business stakeholders are the individuals or groups who have an interest or influence in the organization's activities and outcomes.

By involving business stakeholders in approving the IT strategy, the organization can ensure that the IT strategy reflects and supports the business needs, expectations, and priorities. The other options do not necessarily indicate that IT strategy is aligned with organizational goals and objectives, as they do not involve the participation or feedback of business stakeholders.

References: CISAReview Manual, 27th Edition, page

最新問題: 953

組織の全体的なリスク管理戦略において、ビジネスインパクトアナリスト (BIA)の主な目的は次のうちどれですか？

- A. 組織にとっての事業投資機会の評価
- B. 復旧作業の優先順位付けを効果的に行うために、重要な業務プロセスを特定する。
- C. 定期的な監査を通じて規制遵守を確保する
- D. ネットワークセキュリティ対策を強化するための脆弱性評価の実施

Answer: B ([メッセージを残す](#))

最新問題: 954

次のうち、インシデント管理の主要な目的はどれですか？

- A. 重要度に基づいたサービス復旧
- B. 個々の事案を管理職に報告する
- C. 事件の根本原因の特定
- D. インシデントの原因となったプログラムを修復する

Answer: A ([メッセージを残す](#))

包括的かつ詳細な説明：

インシデント管理の主な目的は、業務の重要度に基づいてITサービスを可能な限り迅速に復旧させ、業務の中断を最小限に抑えることです。

* 根本原因分析 (C)は、インシデント管理ではなく、問題管理により近いものです。

* インシデント (B)の報告は重要ですが、主要な目的ではありません。

* プログラムの修復 (D)は是正活動であり、中心的な目標ではありません。

ISACA 参考資料: CISA レビュー マニュアル第 27 版、ドメイン 2 (IT 運用と事業継続性)、ITIL インシデント管理プロセスに関するセクション。

最新問題: 955

Which of the following is the BEST control to help ensure the completeness of outbound transactions?

- A. Perform edit checks to identify erroneous, unusual, or invalid transactions.
- B. Verify transactions are sequentially numbered in the header record.
- C. Ensure the validity of the recipient ID and use auto-numbered reports.
- D. Maintain a log of the number of messages sent and validate periodically.

Answer: D ([メッセージを残す](#))

Comprehensive and Detailed Step-by-Step Explanation:

To ensure completeness of outbound transactions, along with periodic validation is the best control.

* Option A (Incorrect): Edit checks help with data accuracy, not completeness.

* Option B (Incorrect): Sequential numbering detects missing transactions but does not verify actual transmission.

* Option C (Incorrect): Recipient ID validation is important for accuracy, not for ensuring all transactions are sent.

* Option D (Correct): Maintaining and validating transaction logs ensures that all outbound transactions are properly accounted for, making it the best completeness control.

Reference: ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Covers data integrity, completeness controls, and transaction logging.

最新問題: 956

プログラムの緊急変更に関する手順をレビューする際、IS監査担当者は、手順が以下のとおりであることを確認する必要があります。

- A. 事後フォローアップによって完了する変更を許可します。
- B. 文書化されていない変更を本番ライブラリに直接適用することを許可する。
- C. 緊急の変更は一切認めない。
- D. プログラマーに本番プログラムへの永続的なアクセス権を与える。

Answer: A ([メッセージを残す](#))

システムの問題を解決するために、緊急修正が必要となる場合があります。これには、緊急時にプログラマーが本番プログラムに一時的にアクセスできるようにする特別なログオンIDの使用が含まれます。緊急変更は、事後的なフォローアップ手順を使用して完了する必要があります。これにより、通常の手順が遡及的に適用されることが保証されます。そうしないと、本番環境に影響が出る可能性があります。このようにして行われた変更は、緊急ライブラリに保管し、通常の変更管理プロセスに従って本番ライブラリに移動する必要があります。プログラマーは本番ライブラリを直接変更してはならず、また、本番プログラムへの永続的なアクセス権も付与されてはなりません。

最新問題: 957

When evaluating the ability of a disaster recovery plan (DRP) to enable the recovery of IT processing capabilities, it is MOST important for the IS auditor to verify the plan is:

- A. communicated to department heads,
- B. regularly reviewed.
- C. 外部の場所に保管されます。
- D. 定期的に検査済み。

Answer: D ([メッセージを残す](#))

最新問題: 958

.What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information? Choose the BEST answer.

- A. Referential integrity controls
- B. Normalization controls
- C. Concurrency controls
- D. Run-to-run totals

Answer: ([解答を表示する](#)**)**

Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

最新問題: 959

A database administrator (DBA) should be prevented from having end user responsibilities:

- A. having end user responsibilities
- B. accessing sensitive information

- C. having access to production files
- D. using an emergency user ID

Answer: A ([メッセージを残す](#))

A database administrator (DBA) should be prevented from having end user responsibilities to avoid a conflict of interest and a violation of the principle of segregation of duties. End user responsibilities may include initiating transactions, authorizing transactions, recording transactions or reconciling transactions. A DBA who has end user responsibilities may compromise the integrity, confidentiality and availability of the data and the database systems. Accessing sensitive information, having access to production files and using an emergency user ID are not end user responsibilities, but rather potential risks or controls associated with the DBA role. References:

- * : Database Administrator (DBA) Definition
- * : Segregation of Duties | ISACA
- * : [End User Definition]

最新問題: 960

An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

- A. reclassify the data to a lower level of confidentiality
- B. require the business owner to conduct regular access reviews.
- C. implement a strong password schema for users.
- D. recommend corrective actions to be taken by the security administrator.

Answer: B ([メッセージを残す](#))

The best recommendation for an IS auditor who finds that one employee has unauthorized access to confidential data is to require the business owner to conduct regular access reviews. Access reviews are periodic assessments of user access rights and permissions to ensure that they are appropriate, necessary, and aligned with the business needs and objectives. Access reviews help to identify and remediate any unauthorized, excessive, or obsolete access that could pose a security risk or violate compliance requirements.

The business owner is responsible for defining and approving the access requirements for their data and ensuring that they are enforced and monitored. References:

- * CISA Review Manual (Digital Version)
- * CISA Questions, Answers & Explanations Database

最新問題: 961

ネットワークパフォーマンスに関する以下の記述のうち、誤っているものを特定してください。

- A. 帯域幅 - 帯域幅は一般的にビット/秒で測定され、情報を転送できる最大速度です。
- B. レイテンシ - レイテンシとは、情報が実際に転送される速度のことです。
- C. ジッター - 情報が受信側に到達するまでの時間のジッター変動
- D. エラー率 - エラー率とは、送信された全ビット数に対する破損ビット数をパーセンテージまたは分数で表したものです。

Answer: (解答を表示する)

説明／参考資料：

問題文の中で使われているキーワードは「INCORRECT」です。ネットワークパフォーマンスについて誤って説明されている記述を見つける必要があります。スループットとは実際に情報が転送される速度であり、レイテンシとは送信者と受信者が情報を復号化するまでの遅延です。これは主に信号の伝送時間と、情報が通過するすべてのノードでの処理時間の関数です。試験では、ネットワークパフォーマンスについて以下の情報を知っておく必要があります。

ネットワークパフォーマンスとは、顧客から見た通信製品のサービス品質を測定することを指します。

以下に、回線交換ネットワークとパケット交換ネットワークの一種（ATM）におけるネットワーク性能指標の例を示します。

回線交換ネットワーク：回線交換ネットワークでは、ネットワーク性能はサービス品質と同義です。拒否された通話の数は、トラフィック負荷が高い状況下でのネットワークの性能を示す指標となります。その他の性能指標としては、ノイズ、エコーなどが挙げられます。

ATM：非同期転送モード（ATM）ネットワークでは、パフォーマンスは回線速度、サービス品質（QoS）、データスループット、接続時間、安定性、技術、変調方式、モデムの機能強化によって測定できます。

ネットワークの特性や設計はそれぞれ異なるため、ネットワークのパフォーマンスを測定する方法は多岐にわたります。パフォーマンスは測定する代わりにモデル化することも可能です。その一例として、状態遷移図を用いて回線交換ネットワークにおける待ち行列のパフォーマンスをモデル化する方法があります。これらの図を用いることで、ネットワーク設計者は各状態におけるネットワークのパフォーマンスを分析し、ネットワークを最適に設計することができます。

以下の対策はしばしば重要視される。

帯域幅 - 帯域幅は一般的にビット/秒で測定され、情報を転送できる最大速度です。

スループット - スループットとは、情報が実際に転送される速度のことです。レイテンシ - レイテンシとは、送信者と受信者が情報を復号化するまでの遅延のことです。これは主に信号の伝搬時間と、情報が通過するすべてのノードでの処理時間の関数です。ジッタ - ジッタとは、情報が受信者に到着するまでの時間の変動のことです。エラー率 - エラー率とは、送信されたビット総数に対する破損ビットの割合または分数で表される、破損したビットの数のことです。

以下の回答は誤りです。

他の選択肢は、ネットワークのパフォーマンスパラメータを正しく説明しています。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版、275ページ

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **962**

A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed Which of the following is the MOST important requirement to include In the vendor contract to ensure continuity?

- A. Continuous 24/7 support must be available.
- B. The vendor must have a documented disaster recovery plan (DRP) in place.
- C. Source code for the software must be placed in escrow.

D. The vendor must train the organization's staff to manage the new software

Answer: C ([メッセージを残す](#))

Explanation

Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training.

References:

CISA Review Manual (Digital Version), Chapter 5, Section 5.51

CISA Review Questions, Answers & Explanations Database, Question ID 228

最新問題: 963

侵入者がアプリケーションサーバーにアクセスし、システムログに変更を加えた。以下のうち、変更を特定できるのはどれか？

- A.** システムログを別のサーバーにミラーリングする
- B.** システムログを書き込み専用ディスクに同時に複製する
- C.** システムログを含むディレクトリを書き込み禁止にする
- D.** システムログのバックアップをオフサイトに保存する

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

書き込み専用CDは上書きできません。そのため、ディスク上に複製されたシステムログを元のログと比較することで、侵入者による変更の可能性のある差異を検出できます。システムログを書き込み保護しても、スーパーユーザーが書き込み保護を解除できるため、削除や変更は防止できません。バックアップやミラーリングによって以前のファイルが上書きされる場合があり、最新の状態ではない可能性があります。

最新問題: 964

Which of the following is the MOST appropriate and effective fire suppression method for an unstaffed computer room?

- A.** Fire extinguishers
- B.** Carbon dioxide (CO2)
- C.** Water sprinkler
- D.** Dry pipe

Answer: B ([メッセージを残す](#))

最新問題: 965

What would be an IS auditor's BEST recommendation upon discovering that consumer records in a database have not been protected?

- A.** Implement security event log reviews.
- B.** Ensure database patches are installed.

- C. Implement access controls.
- D. Encrypt the data in the database.

Answer: C ([メッセージを残す](#))

最新問題: 966

電気配線、空調設備、床材は備えているが、コンピュータや通信機器がないオフサイトの情報処理施設は、次のうちどれに該当するか。

- A. 低温サイト。
- B. 暖かい場所。
- C. ダイヤルアップサイト。
- D. 複製処理施設。

Answer: A ([メッセージを残す](#))

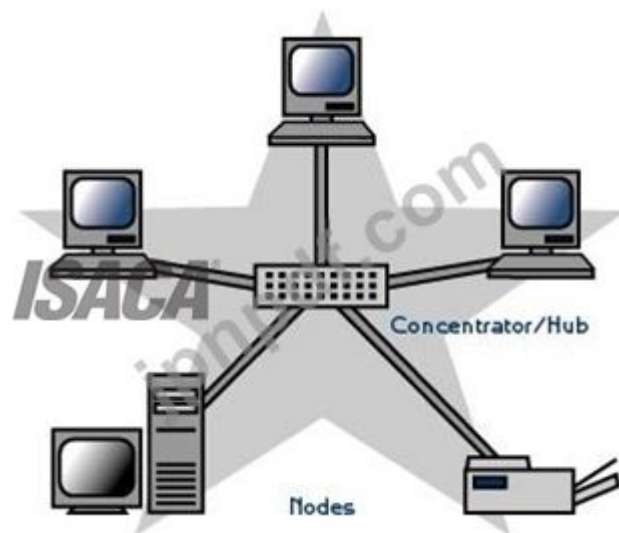
コールドサイトは機器を受け入れる準備はできているが、事前にサイトに部品を提供することはない。必要性の。

不正解：

- B. ウォームサイトとは、情報処理施設を運用するために、ネットワーク接続や、ディスクやテープユニット、コントローラ、CPUなどの選択された周辺機器が部分的に構成されたオフサイトのバックアップ施設です。
- D. 複製情報処理施設は、重要なアプリケーションをバックアップできる専用の自社開発の復旧サイトです。

最新問題: 967

下記の図からネットワークトポロジーを特定してください。



ネットワークトポロジー

- A. バス
- B. スター
- C. リング
- D. メッシュ

Answer: B ([メッセージを残す](#))

説明／参考資料：

試験では、LANトポロジーに関する以下の情報を理解しておく必要があります。

LANトポロジー

ネットワークトポロジーとは、コンピュータネットワークを構成する様々な要素（リンク、ノードなど）の物理的な配置のことである。

本質的に、これはネットワークのトポロジー構造であり、物理的または論理的に表現できます。物理的トポロジーは、デバイスの配置やケーブルの配線など、ネットワークのさまざまなコンポーネントの配置を指し、論理的トポロジーは、物理的な設計に関係なく、ネットワーク内でデータがどのように流れるかを示します。

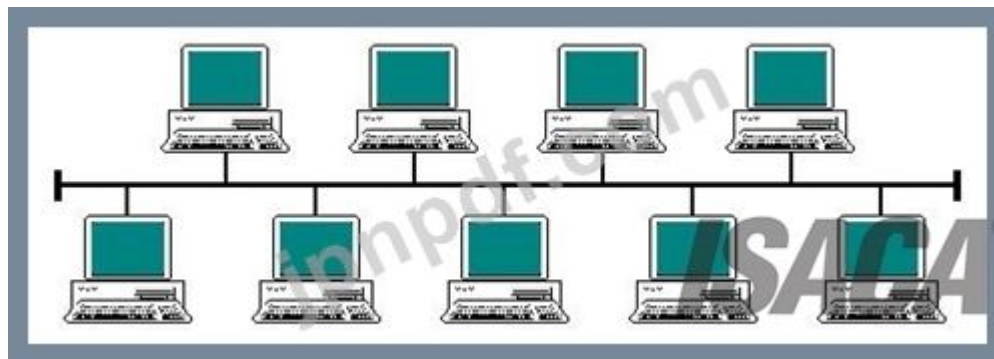
ノード間の距離、物理的な相互接続、伝送速度、および／または信号の種類は、2つのネットワーク間で異なる場合があるが、トポロジーは同一である可能性がある。

バス

バス型トポロジーを採用したローカルエリアネットワークでは、各ノードは1本のケーブルに接続されます。各コンピュータまたはサーバは、1本のバスケーブルに接続されます。送信元からの信号は、バスケーブルに接続されているすべてのマシンに双方向に伝送され、目的の受信者を見つけます。マシンのアドレスがデータの宛先アドレスと一致しない場合、マシンはそのデータを無視します。逆に、データがマシンのアドレスと一致する場合は、データは受け入れられます。バス型トポロジーは1本のワイヤのみで構成されるため、他のトポロジーと比較して実装コストはかなり安価です。しかし、この技術の実装コストの低さは、ネットワーク管理コストの高さによって相殺されます。さらに、使用されるケーブルが1本だけであるため、単一障害点となる可能性があります。ネットワークケーブルの両端が終端処理されておらず、終端処理がない場合、データ転送が停止し、ケーブルが断線すると、ネットワーク全体がダウンします。

バストポロジー

画像提供元：



http://www.technologyuk.net/telecommunications/networks/images/bus_topology.gif 直線バス

ネットワークのすべてのノードが、正確に2つのエンドポイントを持つ共通の伝送媒体（これは「バス」と呼ばれ、一般的にバックボーンまたはトランクとも呼ばれる）に接続されているネットワークトポロジーのタイプ。ネットワーク内のノード間で送信されるすべてのデータは、この共通の伝送媒体を介して送信され、ネットワーク内のすべてのノードで同時に受信できます。

分散バス

ネットワークのすべてのノードが共通の伝送媒体に接続され、伝送媒体のメインセクションにブランチを追加することによって作成される2つ以上のエンドポイントを持つネットワークトポロジーのタイプ。物理的分散バストポロジーは、物理的線形バストポロジーとまったく同じように機能します（つまり、すべてのノードが共通の伝送媒体を共有します）。

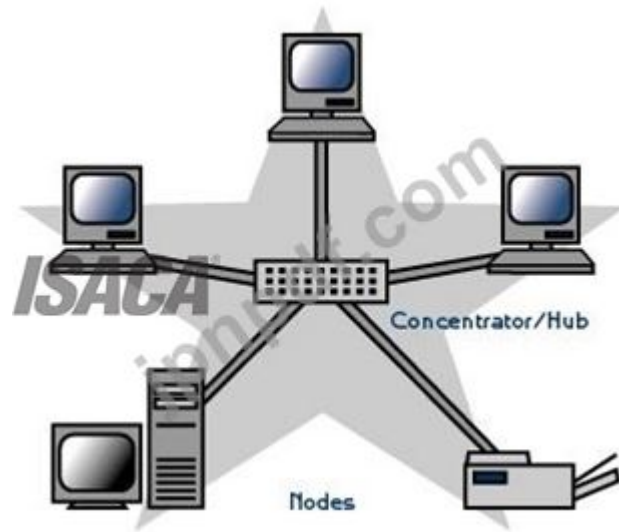
星

スター型トポロジーのローカルエリアネットワークでは、各ネットワークホストはポイントツーポイント接続で中心点に接続されます。スター型トポロジーでは、すべてのノード（コンピュータワークステーションやその他の周辺機器）がハブまたはスイッチと呼ばれる中心ノードに接続されます。

スイッチはサーバーであり、周辺機器はクライアントである。ネットワークは必ずしも星型である必要はないが、ネットワーク上のすべてのノードは1つの中央デバイスに接続されている必要がある。

ネットワークを通過するすべてのトラフィックは、中央ポイントを経由します。中央ポイントは信号中継器として機能します。スター型トポロジーは、設計と実装が最も容易なトポロジーと考えられています。スター型トポロジーの利点は、ノードの追加が容易であることです。一方、最大の欠点は、中心点が単一障害点となることです。

スター型トポロジー



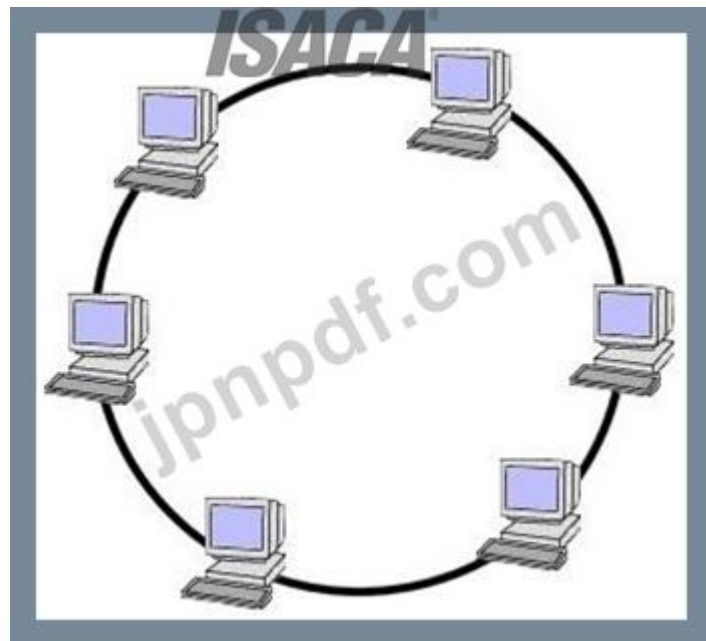
画像出典 <http://fcit.usf.edu/network/chap5/pics/star.gif>

指輪

データが一方向にリングを周回する円形ネットワークトポロジー。リング上の各デバイスはリピーターとして機能し、信号強度を維持します。各デバイスには、受信信号を受信する受信機と、データをリング内の次のデバイスに送信する送信機が内蔵されています。

このネットワークは、信号がリング内を伝送できる能力に依存しています。デバイスがデータを送信する際、データは宛先に到達するまでリング上のすべてのデバイスを経由する必要があります。すべてのノードは重要なリンクです。いずれかのノードがダウンすると、リンク全体に影響が出ます。

リングトポロジー



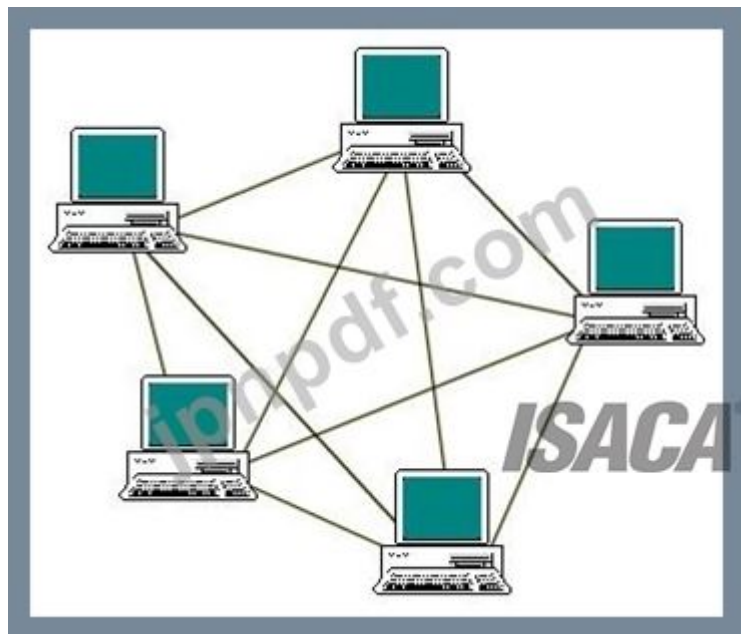
画像出典 <https://forrester-infosystems.wikispaces.com/>

メッシュ

完全メッシュネットワークの価値は、加入者数の指数に比例する。ただし、通信する任意の2つのエンドポイントのグループ 全てのエンドポイントを含む)は、リードの法則によって近似されると仮定する。

メッシュネットワークは、高い可用性と冗長性を提供します。しかし、メッシュネットワークに数十台のデバイスが接続される場合、そのコストは非常に高額になる可能性があります。

メッシュトポロジー



画像出典 http://www.technologyuk.net/telecommunications/networks/images/mesh_topology.gif 完全接続型メッシュトポロジー
完全接続ネットワークとは、各ノードが互いに接続されている通信ネットワークのことです。グラフ理論では、完全グラフと呼ばれます。完全接続ネットワークは、スイッチングやブロードキャストを必要としません。しかし、接続数がノード数の2乗に比例して増加するため、大規模ネットワークには極めて不向きであるという大きな欠点があります。2ノードネットワークは、厳密には完全接続ネットワークです。

部分的に連結されたメッシュトポロジー

ネットワークのノードの一部が、ポイントツーポイントリンクによってネットワーク内の他の複数のノードに接続されているタイプのネットワークトポロジー。これにより、ネットワーク内のすべてのノード間を接続するために必要なコストと複雑さを伴うことなく、物理的に完全に接続されたメッシュトポロジーによって提供される冗長性の一部を活用することが可能になります。

以下の回答は誤りです。

提示された他の選択肢は無効です。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014、262ページ

最新問題: 968

コントロール自己評価 (CSA) を使用する上で最も重要な利点は次のうちどれですか？

- A. より効果的で改善された内部統制
- B. 従業員の参加による結束力のあるチームの構築
- C. 所有権の明確化
- D. リスクの早期発見

Answer: D ([メッセージを残す](#))

自己評価による管理策（CSA）の最も重要な利点は、リスクを早期に発見できることです。CSAによって、プロセスオーナーは管理策の有効性を定期的に評価することができ、重大な問題に発展する前に弱点や新たなリスクを特定するのに役立ちます。

最新問題: 969

One advantage of monetary unit sampling is the fact that:

- A. large-value population items are segregated and audited separately
- B. results are stated in terms of the frequency of items in error
- C. it increases the likelihood of selecting material items from the population,
- D. it can easily be applied manually when computer resources are not available

Answer: C ([メッセージを残す](#))

最新問題: 970

組織のITセキュリティポリシーでは、全従業員を対象とした年次のセキュリティ意識向上トレーニングが義務付けられています。トレーニングの効果を最もよく示す証拠となるのは、次のうちどれでしょうか？

- A. ソーシャルエンジニアリングテストの結果
- B. 従業員へのインタビュー
- C. インシデント対応チームへの電話件数の減少
- D. 無作為に選ばれた従業員が回答したアンケート

Answer: A ([メッセージを残す](#))

セクション :ITのガバナンスと管理

最新問題: 971

ビジネスインパクト分析（BIA）の後に行うべき活動は次のうちどれですか？

- A. IT環境に対する脅威を特定する
- B. 重要なアプリケーションを特定する
- C. 復旧オプションの分析
- D. コンピューティング環境とユーザー環境をレビューする

Answer: C ([メッセージを残す](#))

セクション : 情報システムの取得、開発、導入

最新問題: 972

コントロール自己評価（CSA）手法を採用する組織から得られる主なメリットは、CSA です。

- A. 詳細なレビューが必要な高リスク領域を特定できます
- B. 従来の監査の代替として使用できます
- C. 経営陣が管理責任を放棄できるようにする
- D. IS監査人がリスクを独立して評価できるようにする

Answer: ([解答を表示する](#)**)**

最新問題: 973

Which of the following would be of GREATEST concern to an IS auditor evaluating an organization's change management process?

- A. Change management meeting minutes are not available for several meetings.
- B. Change requests are not subject to prioritization.
- C. Changes are approved after being moved to production.
- D. A list of authorized requestors for emergency changes does not exist.

Answer: C ([メッセージを残す](#))

The best answer is C. Changes are approved after being moved to production.

ISACA guidance on change management emphasizes reviews, testing, approvals, and segregation of duties before moving changes forward. If changes are moved into production before approval, the organization has effectively bypassed one of the most important preventive controls in the change process. That creates direct risk of unauthorized, untested, or harmful changes reaching production.

Option A is a documentation weakness. Option B reduces efficiency and prioritization discipline. Option D is a concern for emergency changes, but it is still less severe than routinely approving changes only after implementation. In audit terms, post-production approval represents a fundamental control breakdown.

References (Official ISACA):

* ISACA Journal, Speeding Up Software Delivery With Effective Change Management.

最新問題: 974

Which of the following is a concern in an enterprise architecture (EA) program?

- A. The architecture review board is chaired by the CIO
- B. IT application owners have sole responsibility for architecture approval
- C. The EA program governs projects that are not IT-related
- D. Information security requirements are reviewed by the EA program

Answer: B ([メッセージを残す](#))

Comprehensive and Detailed In-Depth Explanation: IT application owners having sole responsibility for architecture approval (B) is a major concern because it indicates a lack of oversight and segregation of duties.

EA decisions should be reviewed by a cross-functional governance body to ensure alignment with security, compliance, and business objectives.

Other options:

- * The CIO chairing the review board (A) may indicate centralized leadership but is not inherently a risk.
- * EA governing non-IT projects (C) may indicate scope expansion but is not a security risk.
- * Security requirements being reviewed (D) is a best practice and not a concern.

Reference: ISACA CISA Review Manual, IT Governance and Management of IT

最新問題: 975

IS監査担当者がオペレーティングシステムのアップグレードをレビューしています。次のうちどれが最大の監査上の懸念事項は？

- A. リリースノートがない
- B. 変更管理の欠如
- C. マルウェア対策の欠如

D. 活動記録の欠如

Answer: ([解答を表示する](#))

セクション：情報システムの監査プロセス

最新問題: **976**

Which of the following should an IS auditor consider the MOST significant risk associated with a new health records system that replaces a legacy system?

- A.** Staff were not involved in the procurement process, creating user resistance to the new system.
- B.** Data is not converted correctly, resulting in inaccurate patient records.
- C.** The deployment project experienced significant overruns, exceeding budget projections.
- D.** The new system has capacity issues, leading to slow response times for users.

Answer: B ([メッセージを残す](#))

The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection.

Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as significant as data not being converted correctly. References: [ISACA CISA Review Manual 27th Edition], page 281.

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **977**

Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

- A.** Review software migration records and verify approvals.
- B.** identify changes that have occurred and verify approvals.
- C.** Review change control documentation and verify approvals.
- D.** Ensure that only appropriate staff can migrate changes into production.

Answer: ([解答を表示する](#))

Explanation/Reference:

Explanation:

The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

最新問題: 978

情報システム監査担当者が、組織のソフトウェア開発ライフサイクルに関する方針に不備があることを指摘した。次に行うべきことはどれですか？

- A. 監査報告書に調査結果を記載する。
- B. 誰がポリシーを承認したかを特定する。
- C. 状況を主任監査員に報告する。
- D. 観察結果を被監査者に伝える。

Answer: D (メッセージを残す)

IS監査担当者は、組織のソフトウェア開発ライフサイクル (SDLC) ポリシーに不備があることを特定しました。SDLCとは、ソフトウェアアプリケーションの計画、開発、テスト、および展開のプロセスです¹。SDLCポリシーとは、SDLCプロセスを統制し、その品質、セキュリティ、およびコンプライアンスを保証するガイドラインと標準です²。SDLCポリシーの不備は、次のようなさまざまなリスクにつながる可能性があります。

* アプリケーションの機能、信頼性、またはセキュリティに影響を与える可能性のあるソフトウェアのエラー、バグ、または脆弱性³

* ソフトウェアの障害、遅延、または超過により、アプリケーションの提供、パフォーマンス、または顧客満足度に影響が生じる可能性があります。³

* 法的、規制的、または契約上の違反や罰則につながる可能性のあるソフトウェアの不適合³ SDLC ポリシーの不備を特定した後、IS 監査人が次に行うべきことは、監査対象者にその所見を伝えることです。監査対象者とは、監査の対象となる個人または組織であり、監査対象領域に責任を負っています⁴。この場合、監査対象者は、ソフトウェア開発マネージャー、プロジェクトマネージャー、または組織の上級管理職である可能性があります。監査対象者に所見を伝えることは、いくつかの理由から重要です。

* これにより、IS監査人は観察結果の正確性と妥当性を検証し、被監査者から追加の証拠や情報を収集することができます。⁴

* 監査対象者は、指摘事項に対して回答し、不備に対する見解、説明、または正当化を提供する機会を得る。⁴

* これにより、IS監査担当者は被監査企業と、欠陥の潜在的な影響、根本原因、および是正計画について話し合うことができる。⁴

* IS監査人と被監査者との間で協力的かつ建設的な関係が促進され、監査プロセスにおける透明性と説明責任が高まります。⁴ 他の選択肢は、被監査者に観察結果を伝えるほど適切ではありません。監査報告書に調査結果を文書化するのは、被監査者とコミュニケーションを取り、観察結果を確定した後に行うべき後のステップです。ポリシーを承認した人物を特定することは、欠陥に対処する上で重要ではなく、特定の個人またはグループに責任や過失があることを意味する可能性があります。被監査者との間で通常のコミュニケーションでは解決できない深刻な意見の相違や対立がない限り、状況を主任監査人にエスカレートする必要はありません。したがって、選択肢Dが正解です。

参考文献：

* ソフトウェア開発ライフサイクルとは？ | PagerDuty

* ソフトウェア開発ライフサイクル (SDLC) ポリシー | StrongDM

* SDLCとは何か？最適なフェーズ、方法論、そしてメリットを明らかに - ケルトン

監査結果の伝達

最新問題: 979

Which of the following areas is MOST likely to be overlooked when implementing a new data classification process?

- A. End-user computing (EUC) systems
- B. New system applications
- C. Data sent to vendors
- D. Email attachments

Answer: [\(解答を表示する\)](#)

最新問題: 980

.Which of the following provides the strongest authentication for physical access control?

- A. Sign-in logs
- B. Dynamic passwords
- C. Key verification
- D. Biometrics

Answer: D ([メッセージを残す](#))

Biometrics can be used to provide excellent physical access control.

最新問題: 981

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

- A. test the software for compatibility with existing hardware.
- B. perform a gap analysis.
- C. review the licensing policy.
- D. ensure that the procedure had been approved.

Answer: D ([メッセージを残す](#))

Section: Protection of Information Assets

Explanation:

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

最新問題: 982

事業継続性に関する以下の用語のうち、システムおよび／またはデータの整合性を検証するために必要な許容最大時間を決定するものはどれですか？

- A. RPO
- B. RTO
- C. WRT
- D. MTD

Answer: C ([メッセージを残す](#))

説明／参考資料：

作業復旧時間 (WRT)は、システムおよび／またはデータの整合性を検証するために必要な許容最大時間を決定します。これには、例えば、データベースやログの確認、アプリケーションやサービスが稼働していて利用可能であることを確認する作業などが含まれます。ほとんどの場合、これらの作業はアプリケーション管理者やデータベース管理者などが行います。災害の影響を受けたすべてのシステムが検証および／または復旧されると、環境は本番環境を再開する準備が整います。試験を受けるにあたっては、RPO、RTO、WRT、MTDIに関する以下の情報を知っておく必要があります。

ステージ1：通常業務

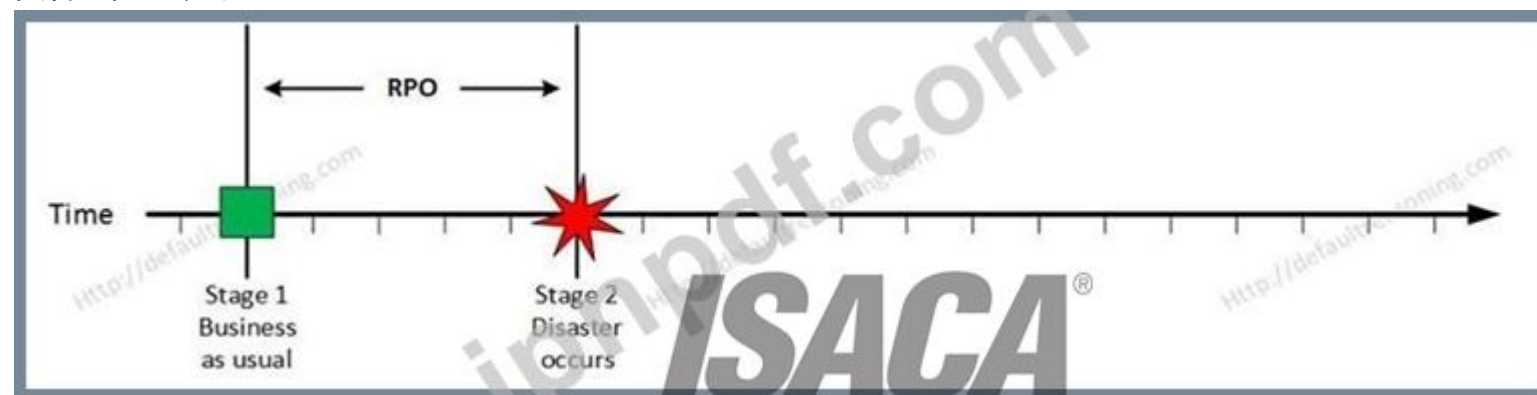
通常通り営業



画像参照 - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-01.png> 現段階では、すべてのシステムが本番稼働しており、正常に動作しています。

ステージ2：災害発生

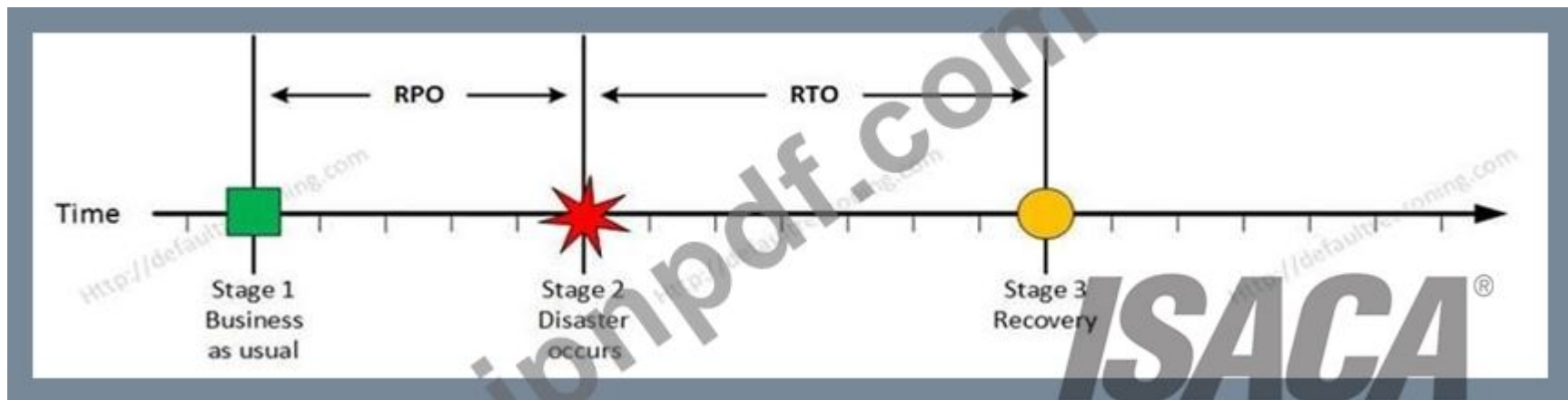
災害が発生する



画像参照 - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-02.png> ある時点で災害が発生し、システムの復旧が必要になります。この時点で、リカバリポイント目標 (RPO)は、時間で測定される許容可能な最大データ損失量を決定します。たとえば、許容可能な最大データ損失は15分です。

ステージ3：回復

回復



画像参照 - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-03.png> この段階では、システムは復旧してオンラインに戻っていますが、まだ運用準備は整っていません。リカバリ時間目標 (RTO) は、すべての重要なシステムをオンラインに戻すために必要な許容可能な最大時間を決定します。これには、たとえば、バックアップからのデータ復元や障害の修復が含まれます。ほとんどの場合、この部分はシステム管理者、ネットワーク管理者、ストレージ管理者などが実行します。

ステージ4：履歴書の作成

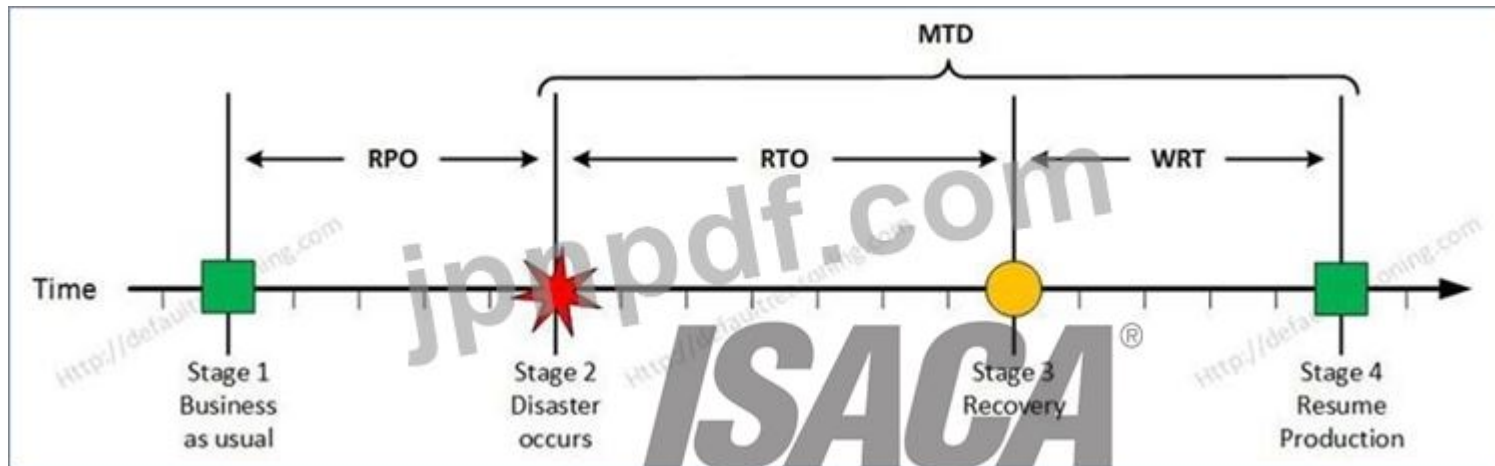
履歴書作成



画像参照 - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-04.png> この段階では、すべてのシステムが復旧し、システムまたはデータの整合性が検証され、すべての重要なシステムが通常の動作を再開できます。作業復旧時間 (WRT) は、システムおよび/またはデータの整合性を検証するために必要な許容可能な最大時間を決定します。これには、たとえば、データベースとログの確認、アプリケーションまたはサービスが実行されて利用可能であることを確認することなどが含まれます。

ほとんどの場合、これらの作業はアプリケーション管理者やデータベース管理者などによって実行されます。災害の影響を受けたすべてのシステムが検証および/または復旧されると、環境は再び運用を再開できる状態になります。

MTD



画像参照 - <http://defaultreasoning.files.wordpress.com/2013/12/bcdr-05.png> RTOとWRTの合計は、許容最大ダウンタイム (MTD) として定義され、ビジネスプロセスが許容できない結果を引き起こすことなく中断できる合計時間を示します。この値は、経営陣、またはCTO、CIO、ITマネージャーなどの担当者が定義する必要があります。

以下の回答は誤りです。

RPO (リカバリポイント目標)とは、許容できるデータ損失の最大許容時間を時間単位で定義したものです。例えば、許容できるデータ損失の最大時間は15分です。

RTO (リカバリ時間目標)とは、すべての重要システムをオンラインに戻すために必要な許容最大時間を決定するものです。これには、例えば、バックアップからのデータ復元や障害の修復などが含まれます。

ほとんどの場合、この部分はシステム管理者、ネットワーク管理者、ストレージ管理者などが担当します。

MTD (最大許容ダウンタイム)とは、RTO (復旧時間)とWRT (復旧時間の合計であり、業務プロセスが中断しても許容できない結果が生じない合計時間を指します。この値は、経営陣、CTO (最高技術責任者)、CIO (最高情報責任者)、ITマネージャーなどの担当者が設定する必要があります。

この質問を作成するにあたり、以下の参考文献が使用されました。

CISAレビューマニュアル2014年版、284ページ

<http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/>

最新問題: 983

組織が顧客信用審査システムを第三者サービスプロバイダーにアウトソーシングする場合、IS監査において最も重要な考慮事項は次のうちどれですか？プロバイダー：

- A. 業界のセキュリティ基準を満たしているか、それを上回っています。
- B. 外部のセキュリティ審査を受けることに同意する。
- C. サービスと経験において市場で高い評価を得ています。
- D. 組織のセキュリティポリシーに準拠している。

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

顧客の信用情報がアウトソーシング先に保管されるため、アウトソーシング先のベンダーに対する独立したセキュリティレビューを取得することが極めて重要です。セキュリティ基準や組織方針への準拠は重要ですが、独立したレビューなしにそれが事実であることを検証または証明する方法はありません。長年の事業経験と高い評判はサービス品質を評価する上で重要な要素ですが、セキュリティ管理が脆弱なプロバイダーにアウトソーシングすることはできません。

最新問題: 984

データ編集は処理前に実施され、次のうちどれに該当しますか？最適な回答を選択してください。

- A. 抑止力の完全性管理
- B. 探偵の整合性管理
- C. 是正措置による完全性管理
- D. 予防的完全性管理

Answer: D ([メッセージを残す](#))

データ編集は処理前に実施され、予防的な整合性管理とみなされます。

最新問題: 985

コンピュータのパフォーマンスを分析する際に、次のうちどれが最も役立つでしょうか？

- A. 応答時間に対するユーザーの不満に関する運用報告
- B. オフピーク時の利用状況と応答時間の報告
- C. システムソフトウェアの調整によるリソース使用量の最適化
- D. 設備稼働率を測定する統計指標

Answer: A ([メッセージを残す](#))

最新問題: 986

ある組織は、業務量の増加に伴う需要に対応するため、メインフレームコンピュータの交換を購入しました。情報システム監査担当者が最も重視すべき事項は次のうちどれでしょうか？

- A. 災害復旧計画は見直し、更新されました。
- B. 適切な入札評価プロセスが遵守されました。
- C. アプリケーションのアクセス制御は適切です。
- D. 調達は、当該年度の計画予算の範囲内です。

Answer: ([解答を表示する](#))

最新問題: 987

組織のIT戦略計画をレビューするIS監査担当者は、まず最初に以下の点をレビューする必要があります。

- A. 既存のIT環境。
- B. 事業計画書
- C. 現在のIT予算。
- D. 現在の技術動向。

Answer: B ([メッセージを残す](#))

セクション：情報資産の保護

Explanation:

IT戦略計画は、組織の事業計画を支援するために存在します。IT戦略計画を評価するには、情報システム監査担当者はまず事業計画の内容を把握する必要があります。

最新問題: 988

IS監査の一環として証拠を評価する際、以下の情報源のうち、最も信頼できるとみなすべきものはどれですか？

- A. 監査人の前で提示された証拠
- B. 第三者から提供された証拠
- C. 被監査者から直接提供された証拠
- D. 上級管理職が厳選した証拠

Answer: B ([メッセージを残す](#))

最新問題: 989

フォローアップ監査のスケジュールを立てる際に、最も重要な考慮事項は次のうちどれですか？

- A. 観測に関連する制御と検出リスク
- B. 被監査企業が監査人と過ごすことに同意した時間
- C. 新規監査人による独立検証に必要な労力
- D. 是正措置が講じられなかった場合の影響

Answer: D ([メッセージを残す](#))

最新問題: 990

An IS auditor finds that confidential company data has been inadvertently leaked through social engineering.

The MOST effective way to help prevent a recurrence of this issue is to implement:

- A. data loss prevention (DIP) software.
- B. a third-party intrusion prevention solution
- C. penalties to staff for security policy breaches
- D. a security awareness program.

Answer: ([解答を表示する](#)**)**

最新問題: 991

IS監査担当者が、外部委託されたヘルプデスクのサービス管理をレビューしています。サービスプロバイダーがこの機能をどれだけ効果的に実行しているかを示す最適な指標は次のうちどれですか？

- A. 処理した通話件数
- B. 平均チケット年齢
- C. 通話記録のレビュー
- D. 顧客満足度評価

Answer: ([解答を表示する](#)**)**

有効な **CISA** 問題集は GoShiken.com が提供された合格しやすい CISA 試験問題集！ GoShiken.com が最新の **CISA** 試験問題集を提供しています。GoShiken.com CISA 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISA 問題集をゲットする人はこちら: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (**156230%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 992

直接切り替え方式で新しい基幹システムへの移行を準備する際に、以下のIS監査結果のうち、最も懸念すべき事項はどれでしょうか？

- A. 一部の重要なレポートのテストケースが不完全です。
- B. 非公式な管理承認を得て本番稼働へ
- C. システム稼働開始時のロールバック戦略の欠如
- D. 稼働開始後、長期間にわたりいくつかの回避策を用いる予定

Answer: C ([メッセージを残す](#))

セクション：情報システムの運用、保守およびサポート

最新問題: 993

IS監査担当者は、組織が質の高いセキュリティポリシーを持っていると結論付けました。次に確認すべき最も重要な事項は次のうちどれですか？ポリシーは次の条件を満たす必要があります。

- A. 全従業員に十分に理解されている。
- B. 業界標準に基づいています。
- C. プロセスオーナーによって開発されました。
- D. 頻繁に更新されます。

Answer: A ([メッセージを残す](#))

組織が質の高いセキュリティポリシーを策定していると結論付けた後、次に最も重要なのは、そのポリシーが全従業員に十分に理解されているかどうかを確認することです。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目的、範囲、役割、責任、および規則を定めた文書です。質の高いセキュリティポリシーとは、明確で簡潔、一貫性があり、包括的で、ビジネス目標や要件に合致しているものです。しかし、質の高いセキュリティポリシーであっても、それを遵守することが求められる全従業員に十分に理解されていなければ意味がありません。したがって、IS監査担当者は、従業員のセキュリティポリシーに対する認識と理解度を評価し、対処すべきギャップや問題点を特定する必要があります。他の選択肢は、セキュリティポリシーの実施と有効性に直接影響しないため、全従業員がセキュリティポリシーを十分に理解していることを確認することほど重要ではありません。

参考文献：CISAレビューマニュアル、第27版、317ページ

最新問題: 994

An IS auditor is reviewing an organization's implementation of a bring your own device (BYOD) program.

Which of following would be the BEST recommendation to help ensure sensitive data is protected if a device is in the possession of an unauthorized individual?

- A. Enable the location service feature on devices.
- B. Encrypt data on devices including storage media.
- C. Authenticate device users when accessing the corporate network.
- D. Enable remote wiping of critical data.

Answer: B ([メッセージを残す](#))

Section: Protection of Information Assets

最新問題: 995

最高情報責任者 (CIO) が、組織のITプロセスとシステムに対して複数のセキュリティ対策を実施するよう情報システム監査人に依頼しました。監査人は以下のことを行うべきです。

- A. 利益相反を監査管理部門に伝える
- B. 適切な専門的注意を払って、業務および今後の監査を実施する。
- C. 実施について経営陣の承認を得る
- D. 独立問題のため拒否。

Answer: A ([メッセージを残す](#))

最新問題: 996

外部監査において、情報システム監査担当者は、組織内でシステムの重要度分類に一貫性がないことに気づきました。システムの重要度を判断するための主たる要素として、次のうちどれを推奨すべきでしょうか？

- A. 最大許容停止時間 (MAD)
- B. 主要業績評価指標 (KPI)
- C. リカバリポイント目標 (RPO)
- D. 平均復旧時間 (MTTR)

Answer: A ([メッセージを残す](#))

最新問題: 997

Which of the following should be the PRIMARY consideration when designing a backup strategy for an online reservation system that requires high availability?

- A. Data classification
- B. Scheduled maintenance
- C. Recovery time objective (RTO)
- D. Recovery point objective (RPO)

Answer: ([解答を表示する](#))

最新問題: 998

An organization recently switched vendors to perform hardware service and maintenance. The new contract specifies a longer response time than the organization's requirement's. Which of the following is the GREATEST risk of this change?

- A. Unexpected downtime may impact key business processes.
- B. There may be an increase of shadow IT occurrences.
- C. Business data may be lost in the event of system failure.
- D. Disaster recovery plans (DRPs) may have increased dependence on the new vendor.

Answer: C ([メッセージを残す](#))

最新問題: 999

データセンターの天井裏に設置すべき最も重要な環境機器は次のうちどれですか？

- A. モーションセンサー
- B. 空気圧センサー
- C. 煙感知器

D. 湿度センサー

Answer: C ([メッセージを残す](#))

Valid CISA Dumps shared by GoShiken.com for Helping Passing CISA Exam! GoShiken.com now offer the **newest CISA exam dumps**, the GoShiken.com CISA exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com CISA dumps with Test Engine here: <https://www.goshiken.com/ISACA/CISA-mondaishu.html> (1562 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)