コースコード：IA-CISM
税込価格：528,000円 (税抜価格：480,000円)
日数：4日間

ここに注目!!

CISM®（公認情報セキュリティマネージャー）とは、情報セキュリティ管理と統制の専門性を証明するISACA®認定の国際資格です。
ランサムウェア被害などによりサイバー攻撃が事業停止に直結する現在、セキュリティはIT部門の技術課題から「経営課題」へと変わりました。
単なる技術的防御にとどまらず、ビジネス目標と連動した防衛戦略を描き、有事の際の危機対応までも指揮できる「経営視点を持つセキュリティ責任者」へと、技術者をステップアップさせる場として、ISACA®の認定パートナーである当社のトレーニングをご活用ください。

・試験問題のイメージやトレーニングで身につく知識の参考としてお役立てください (英語)
CISM® Practice Quiz (ISACA®公式ページ)

・CISM®のほか、キャリアに合わせた各種ISACA®認定トレーニングを提供しています
AAISM™：AIセキュリティ管理
CISA®：情報システム監査
AAIA™：AIを活用した監査・AIシステムの統制
CRISC®：ITリスク管理・システム統制

受講対象者

このトレーニングはこのような方におすすめです。

・ネットワーク管理者やエンジニア、IT管理者、IT監査員など情報セキュリティやITの専門家
・IS/ITセキュリティおよびコントロールの専門知識と経験があり、チームプレーヤーからマネジャーへの転身を目指す方

前提条件/前提知識

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

5年以上の関連業務経験と3年以上の情報セキュリティ管理者としての職務経験を有する情報セキュリティの専門家を対象としています

目的

このコースを修了すると次のことができるようになります。

- 企業の価値創造におけるガバナンスの役割について説明する。
- 企業全体のガバナンスにおける情報セキュリティガバナンスの重要性について説明する。
- 事業体に影響を与える関連する法律、規制、契約上の要件を特定する。
- 事業体のリーダーシップ、構造、文化が情報セキュリティ戦略の有効性に及ぼす影響について説明する。
- 情報セキュリティ戦略がエンタープライズ・リスク・マネジメント(ERM)に及ぼす影響について説明する。
- エンタープライズアーキテクチャ(EA)と効果的なエンタープライズガバナンスの関係を説明する。

- 情報セキュリティ戦略を管理するために使用される一般的なフレームワークと標準を評価する。
- 情報セキュリティ戦略の策定と評価において測定指標が重要である理由について説明する。

- 情報セキュリティリスクの影響を減らすために、リスク評価戦略を適用する。
- 企業が直面する脅威の種類を評価する。
- セキュリティコントロールのベースラインが脆弱性とコントロールの不備分析にどのような影響を及ぼすかについて説明する。
- 情報セキュリティの観点から、リスク処理の適用タイプを区別する。
- リスクとコントロールのオーナーシップが情報セキュリティプログラムに及ぼす影響について説明する。
- 情報セキュリティリスクのモニタリングと報告のプロセスを概説する。

- 情報セキュリティアーキテクチャの目標と目的を説明する。
- 情報セキュリティプログラムを構築するために使用される構成要素とリソースを概説する。
- 情報セキュリティプログラムを構築するために利用できる一般的な情報セキュリティ基準とフレームワークを区別する。
- 情報セキュリティの方針、手順、ガイドラインと企業のニーズを合致させる方法を説明する。
- 情報セキュリティプログラムのロードマップを定義するプロセスについて説明する。
- 進捗状況の追跡と上級管理者への報告に使用される主要な情報セキュリティプログラム指標を概説する。
- コントロールを利用して情報セキュリティプログラムを管理する方法について説明する。
- 情報セキュリティプログラムに対する意識と知識を高めるための戦略を策定する。
- セキュリティプログラムをIT 業務やサードパーティ事業者と統合するプロセスを説明する。
- 重要なセキュリティプログラム情報を利害関係者に伝える。

- インシデント管理とインシデント対応を区別する。
- インシデント対応計画の策定に必要な要件と手順を概説する。
- ビジネスインパクト、継続性、インシデント対応の関係について説明する。
- 災害復旧に関するプロセスと成果について説明する。
- インシデント対応計画を評価する場合の測定指標とテストの影響について説明する。
- インシデントを区分または分類するために使用される技法を特定する。
- 効果的なインシデント管理・対応チームに必要な役割と責任の種類を概説する。
- 企業で利用可能なインシデント管理のツールと技術の種類を区別する。
- インシデントの調査、評価、封じ込めに使用されるプロセスと方法について説明する。
- 主要な利害関係者にインシデントとテストについて通知するために使用される通信と通知の種類を特定する。
- インシデントの根絶と復旧に使用されるプロセスと手順を概説する。
- イベントを文書化する要件と利点について説明する。

アウトライン

ドメイン1 - 情報セキュリティガバナンス

組織の目的と文化

法律、規制、および契約上の要件

組織の構造、役割、および責任

情報セキュリティ戦略の策定

エンタープライズアーキテクチャ

情報ガバナンスフレームワークおよび標準

戦略的計画

ドメイン2 - 情報セキュリティリスク管理

新たなリスクおよび脅威の状況

脆弱性とコントロールの不備分析

リスクアセスメントおよび分析

リスク処理/リスク対応の選択肢

リスクおよびコントロールオーナーシップ

リスクモニタリングおよびレポート

ドメイン3 - 情報セキュリティプログラム

情報セキュリティのアーキテクチャ

情報セキュリティプログラムリソース

情報セキュリティの業界標準とフレームワーク

情報セキュリティポリシー、基準、手続き、およびガイドライン

情報資産の特定および分類

情報セキュリティコントロールの設計および選択

情報セキュリティプログラム評価尺度の策定

情報セキュリティコントロールの導入および統合

情報セキュリティコントロールのテストおよび評価

情報セキュリティ意識向上およびトレーニング

外部サービスの管理

情報セキュリティプログラムの評価尺度、コミュニケーション、および報告

ドメイン4 - インシデント管理

インシデント対応計画

ビジネス・インパクト分析(BIA)

事業継続計画(BCP)

災害復旧計画(DRP)

インシデントの分類/カテゴリ化

インシデント管理のトレーニング、テストと評価

インシデント管理ツールおよび技法

インシデント調査および評価

インシデントの封じ込め方法

インシデント対応コミュニケーション

インシデントの根絶および復旧

インシデント事後レビューの実践