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

トレーニング内容

情報リスクマネジメントに精通したITプロフェッショナル向け

・情報セキュリティプログラム開発
・情報セキュリティプログラム管理
・インシデント管理と対応
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を有し、チームプレーヤーからマネジャーへの転身を目指すITプロフェッショナル。CISM®は、社内外の利害関係者、同僚、規制当局との交流に信頼性と自信を与えることができます。
この資格は、情報セキュリティガバナンス、プログラム開発・管理、インシデント管理、リスク管理の専門知識を示すものです。中途採用の IT プロフェッショナルで、IT セキュリティおよび管理部門の上級管理職を目指している場合、CISM®を取得することで、必要な可視性を得ることができます。

ここに注目!!

ワンポイントアドバイス

本トレーニングに含まれているものは以下の通りです。
・レビューマニュアル（テキスト）※電子版
・問題集 ※電子版
・受験バウチャー ※1回分
上記教材およびバウチャーの有効期限は、受講者の方が最初に教材やバウチャー情報にアクセスしてから12か月間です。

受講対象者

このコースの受講対象者は次の通りです。

・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

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。

CISM®は、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専門家を対象としている。

ISACA®のCISM®（Certified Information Security Manager®）は、情報セキュリティマネジメントの知識と経験を認定する国際的資格であり、日本語名称を『公認情報セキュリティマネージャー』と称します。

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。

・情報セキュリティマネジメントの体系的理解
経営と整合した情報セキュリティ戦略の策定・運用の方法を習得できる
・情報セキュリティガバナンスの確立と維持
セキュリティポリシーの策定、組織体制の構築、責任の明確化などを実施できる
・リスクマネジメントに基づいたセキュリティ対策の企画・運用
情報資産のリスク評価・対応・モニタリングをマネジメント視点で実行できる
・セキュリティインシデントへの対応計画の策定と管理
インシデント対応フロー、監視体制、事後評価のプロセスを構築・運用できる
・情報セキュリティプログラムの開発とマネジメント
各種統制策や教育・訓練を含むセキュリティ施策を体系的に管理できる
・ビジネスとの整合性を重視したセキュリティの推進
経営陣や事業部門と連携し、事業継続性とセキュリティの両立を図れる
・国際的なガイドラインや標準（ISO 27001、NISTなど）の理解と適用
グローバルスタンダードに基づくマネジメント体制を構築・評価できる
・CISM®試験合格に向けた知識の習得と演習
CISM® 4ドメインの出題範囲に沿って、重要ポイントと設問パターンを習得できる

アウトライン

モジュール１ – 情報セキュリティガバナンス
セッションのトピック：
• 企業のガバナンスの概要
• 組織の文化、構造、役割、責任
• 法律、規制および契約上の要件
• 情報セキュリティ戦略
• 情報ガバナンスフレームワークおよび標準
• 戦略的計画
学習目標：
• 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
• 企業のリーダーシップ、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
• 企業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
• 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
• 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
リソース：
• 情報セキュリティプログラムガバナンスの目標と成果
• 企業における一般的な役割
• RACI チャートの例

モジュール 2 – 情報セキュリティリスク管理
セッションのトピック：
• リスクと脅威の状況
• 脆弱性とコントロールの不備分析
• リスクの評価、査定、分析

• 情報リスク対応
• リスクの監視、報告、コミュニケーション
学習目標：
• 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監視と報告のプロセスを概説する
リソース：
• 脆弱性と脅威
• 運用リスクの分類
• リスク登録簿の例
• リスク報告書の例
• リスクシナリオ技法の主な課題
• 典型的なリスク管理の文書化
• リスクコミュニケーション計画

モジュール 3：情報セキュリティプログラムの開発と管理
セッションのトピック：
• IS プログラムの開発とリソース
• IS の標準およびフレームワーク
• IS プログラムロードマップの定義
• IS プログラムの測定指標
• IS プログラム管理
• IS の意識向上とトレーニング
• セキュリティプログラムと IT 業務の統合
• プログラムのコミュニケーション、報告、パフォーマンス管理
学習目標：
• 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可能な一般的な IS 標準とフレームワークを区別する
• IS のポリシー、手順、ガイドラインを企業のニーズに合わせる方法について説明する
• IS 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経営者への報告に使用される主要な IS プログラムの測定指標を概説する
• コントロールを利用して IS 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について説明する
• 重要な IS プログラム情報を関連する利害関係者に伝える
リソース：
• 情報セキュリティプログラムガバナンスの目標と成果
• 代替エンタープライズアーキテクチャフレームワーク
• ポリシー、標準、手順、ガイドライン
• セキュリティプログラムの構成要素チェックリスト
• 情報セキュリティフレームワークの構成要素
• 技術的コントロールの構成要素とアーキテクチャ
• 契約ポイント
• 情報セキュリティ連携責任
• セキュリティ課題の種類
• 情報セキュリティプログラムのパフォーマンス測定
• 情報セキュリティプログラム管理の評価に関する質問事項

モジュール 4：情報セキュリティインシデント管理
セッションのトピック：
• インシデント管理とインシデント対応の概要
• インシデント管理と対応計画

- インシデントの区分化/分類化
- インシデント管理の業務、ツール、技術
- インシデントの調査、評価、封じ込め、コミュニケーション
- インシデントの根絶、復旧、レビュー
- ビジネスインパクトと継続性
- 災害復旧計画
- トレーニング、テスト、評価

学習目標：

- 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
- 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
- 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

リソース：

- インシデント管理の行動計画の各フェーズ
- インシデント対応計画の開発
- SEU-CMU の行動計画フェーズ
- 保険の種類と補償内容
- 復旧サイトの種類
- フォレンジック証拠の法律的側面