コースコード：IA-CRISC
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

組織におけるリスクマネジメント(リスク認識・評価)や情報システムコントロールの設計・導入・運用に携わるITプロフェッショナル向け

・ITプロフェッショナル（情報システム分析・開発・管理）
・リスクマネジメント
・内部統制
・ビジネス分析
・コンプライアンス

ISACA®のCRISC®（Certified in Risk and Information Systems Control®）認定資格は、情報システムに関連するリスクの管理と軽減に携わる専門家のために設計された、世界的に認知された資格です。
CRISC®を取得すると、企業のITリスクを特定、評価、対応するための包括的な知識とスキルを身につけることができ、重要な情報資産の完全性、機密性、可用性を確保する上で極めて重要な役割を果たすことができるようになります。
この認定資格は、リスク管理の専門知識を証明し、進化し続けるサイバーセキュリティとITガバナンスの分野でキャリアアップするための強力な基盤を確立します。

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。

・セキュリティディレクター/マネージャー/コンサルタント
・コンプライアンス／リスク／プライバシーのディレクターおよびマネージャー
・IT監査ディレクター／マネージャー／コンサルタント
・コンプライアンス／リスク／管理スタッフ

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。

CRISC®の前提条件として、受験者は、情報システムの監査、管理、またはセキュリティに関する専門的な実務経験を3年以上有していなければならない。

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。

・ITリスク管理の体系的理解
リスクの特定・評価・対応・モニタリングの各フェーズを理解し、実務に応用できる
・組織のビジネス目標とリスクの整合性を図る
戦略目標に沿ったリスク管理の実行と統制策の提案ができる
・統制の設計・実装・監視
ITリスク軽減のための統制（内部統制・ITガバナンス）を設計し、効果的に実装できる
・ITリスク対応策の優先順位付けと実行
影響度や発生可能性に基づくリスク対応策の意思決定ができる
・情報システム管理における統制の評価
システム導入・運用に伴うリスクを評価し、改善策を提案できる
・国際基準（ISO、NIST、COBIT等）に基づいたフレームワークの理解と適用
グローバルな標準を活用したリスク管理・統制の枠組みを構築できる
・試験合格に必要な知識の習得と演習
CRISC®試験範囲（4ドメイン）に対応した知識をインプットし、演習問題で定着できる

アウトライン

ドメイン1：ITリスクの特定
組織の内部及び外部のビジネス及びIT環境に関する既存の文書を含む情報を収集及びレビューし、ITリスクが組織のビジネス目標及び業務に及ぼす潜在的又は現実的な影響を特定する
ITリスク分析を可能にするために、組織の人員、プロセス及び技術に対する潜在的な脅威及び脆弱性を特定する
入手可能な情報に基づき、ITリスクシナリオの包括的なセットを作成し、ビジネス目標及び業務への潜在的な影響を判断する
ITリスクシナリオの主要な利害関係者を特定し、説明責任の確立を支援する
特定されたITリスクシナリオが確実に説明され、全社的なリスクプロファイルに組み込まれるよう、ITリスク登録簿を確立する
ビジネス目標との整合性を確保するために、シニアリーダー及び主要な利害関係者が定義したリスク選好度及び許容度を特定する
利害関係者がリスクを理解し、リスクを認識する文化を促進するために、リスク認識プログラムの開発に協力し、トレーニングを実施する

ドメイン2：ITリスクアセスメント
組織基準（組織構造、方針、標準、技術、アーキテクチャ、統制など）に基づいてリスクシナリオを分析し、特定されたリスクの可能性と影響を判断する
既存の統制の現状を把握し、ITリスク軽減のための有効性を評価する
リスク及び統制の分析結果をレビューし、ITリスク環境の現状と望ましい状態とのギャップを評価する
リスク所有権が適切なレベルで割り当てられ、責任の所在が明確になるようにする
リスク評価の結果を上級管理者及び適切な利害関係者に伝え、リスクに基づく意思決定を可能にする
リスクアセスメントの結果をリスク登録簿に反映させる

ドメイン3：リスク対応の緩和
リスクオーナーと協議を行い、推奨されるリスク対応を選択し、ビジネス目標と整合させ、情報に基づいたリスク決定を可能にする

リスク対応計画の策定についてリスクオーナーと協議し、又はリスクオーナーを支援し、計画に重要な要素（対応、コスト、目標期日等）が含まれていることを確認する
リスクが許容可能なレベルに管理されるよう、緩和策の設計及び実施又は調整について協議する
明確な責任系統を確立するために、コントロールのオーナーシップが割り当てられるようにする
効率的かつ効果的なコントロールの実行を可能にするために、コントロールのオーナーを支援し、コントロールの手順と文書を作成する
リスク及び経営陣のリスク対応の変化を反映するためにリスク登録簿を更新する
リスク対応がリスクアクションプランに従って実行されたことを検証する

ドメイン4：リスクとコントロールのモニタリングと報告
利用可能なデータに基づき、主要リスク指標（KRI）及び閾値を定義・設定し、リスクの変化を監視できるようにする
主要リスク指標（KRI）を監視・分析し、ITリスクプロファイルの変化や傾向を特定する
ITリスクプロファイルに関連する変化や傾向を報告し、経営陣や関係者の意思決定を支援する
統制実績の測定を可能にするための測定基準および主要業績評価指標（KPI）の特定を促進する
主要業績評価指標（KPI）を監視・分析し、統制環境に関連する変化や傾向を特定し、統制の効率性と有効性を判断する
統制評価の結果をレビューし、統制環境の有効性を判断する
意思決定を可能にするため、全体的なリスクプロファイルおよび統制環境のパフォーマンス、変化、または傾向について、関連する利害関係者に報告する