CISM 実務経験証明書

2017 年以降の CISM 試験に合格した申請者

電子的にこの申請書を記入する場合、アドビリーダーを使用してください。

申請者情報

申請者名: _____ ISACA ID: _____

証明者のための書式への記入方法

上記の申請者は ISACA を通して CISM 認証を申請している。ISACA では申請者の実務経験が、雇用の監督者または管理職によって証明される必要があります。証明者は直近の血縁や拡大家族、または人事部の者であってはなりません。

あなた（証明者）は申請書（ページ A-1）と CISM 実務ドメインと業務内容の申告（ページ V-2）に記述されている申請者の実務経験を立証しなければなりません。

この証明書を提出するため申請者に返却してください。質問がある場合は、ISACA にご連絡ください：
https://support.isaca.org または +1.847.660.5505.

証明者情報

証明者名: _____

会社名: _____ 役職: _____

メールアドレス: _____ 電話番号: _____

証明者への質問

1. ページ A-1 に記述されている申請者の情報セキュリティ管理の実務経験を立証します。*（該当なものをすべてチェック）*：

☐ セクション A：会社 1
☐ セクション A：会社 2
☐ セクション A：会社 3
☐ セクション A：会社 4

2. ページ A-1 セクション B に記述されている申請者の一般情報セキュリティの実務経験を立証します。*（該当なものをすべてチェック）*：

☐ セクション B：会社 1
☐ セクション B：会社 2

3. 私は申請者の以下の役割を務めていました：

☐ 監督　者　☐ マネージャー　☐ 同僚　☐ クライアント

4. セクション A で実務経験を立証する場合、ページ A-1/V-2 に記述されている申請者の業務が、私の知る限り正しいことも立証します。

☐ はい　☐ いいえ

証明者の合意

私の知る限り、ページ V-1 と V-2 の情報が正しく、申請者が情報セキュリティマネージャーとして認められない理由はないと立証します。必要であれば、私は ISACA の上記の情報についての質問に快く回答します。

証明者署名: _____ 日付: _____

CISM 実務経験証明書

2017 年以降の CISM 試験に合格した申請者

電子的にこの申請書を記入する場合、アドビリーダーを使用してください。

実務ドメインの記入方法

申請者は対象となるドメインのすべてあるいは一部の業務を完了したことを確認し、証明者の確証を得る必要があります。

ドメイン 1 - 情報セキュリティガバナンス

情報セキュリティガバナンスのフレームワークと支援プロセスを確立および／または維持し、情報セキュリティ戦略が組織の目標と目的と整合していることを確実にする。

業務内容の申告：

- 組織の目標および目的と整合した情報セキュリティ戦略を確立および／または維持し、情報セキュリティプログラムの確立および／またはその継続する管理をガイドすること。
- 情報セキュリティガバナンスのフレームワークを確立および／または維持し、情報セキュリティ戦略を支援する活動をガイドすること。
- 情報セキュリティガバナンスをコーポレートガバナンスに統合し、組織の目標と目的が情報セキュリティプログラムによって支援されていることを確保すること。
- 情報セキュリティポリシーを確立および維持し、企業の目標および目的と整合した標準、手続き、およびガイドラインの作成をガイドすること。
- 情報セキュリティへの投資をサポートするビジネスケースを作成すること。
- 組織への外部および内部の影響を識別し（例えば、新技術、ソーシャルメディア、業務環境、リスク許容度、法的規制事項、第三者の考察、脅威環境等）、情報セキュリティ戦略によってこれらの要素が対処されることを確実にすること。
- 上級指導者層と他の利害関係者からの継続的な関与を得て、情報セキュリティ戦略を上手に実施できるように支援すること。
- 組織全体の情報セキュリティ責任（例えば、データ所有者、データ保護管理者、エンドユーザ、特権ユーザ、または高リスクユーザ等）と権限体制を定義し、伝達し監視すること。
- 情報セキュリティの評価尺度の確立、監視、評価、報告を行い、情報セキュリティ戦略の有効性に関する正確かつ有意義な情報を経営陣に提供すること。

ドメイン 2 - 情報リスク管理

組織の目標と目的に整合するリスク選好度に基づき、情報リスクを受容レベルで管理する。

業務内容の申告：

- 資産保護のために講じる手段が確実に事業価値に釣り合うようにするために、情報資産分類のプロセスを確立もしくは維持すること。
- 準拠違反のリスクを受容レベルで管理するために、法的、規制、組織、その他の適用条件を特定すること。
- 組織の情報に対するリスクを特定し評価するため、リスク評価、脆弱性評価、脅威分析が一貫して、かつ適切なタイミングで確実に実施されるようにすること。
- 組織のリスク選好度に基づき、受容レベルでリスクを管理するために、適切なリスク対処／対応措置の選択肢を特定、推奨、実施すること。
- 情報セキュリティコントロールが適切で、リスクを受容レベルで効果的に管理しているかどうかを判別すること。
- 組織全体で一貫した包括的な情報リスク管理プログラムを実現するため、情報リスク管理をビジネスプロセスとITプロセス（例えば、システム開発、調達、プロジェクト管理）に統合することを促進すること。
- 既存または新しいリスクシナリオへの変更が特定され適切に管理することを確実にするために、リスクの再評価が必要となることがある内部および外部要因（例えば、重要リスク指標[KRIs]、脅威の状況、地政学的状況、規制の変更）をモニタリングすること。
- リスク管理の意思決定プロセスを促進するため、準拠違反と情報リスクのその他の変更を報告すること。
- 組織の木譲渡目的に対する潜在的な影響の理解を支援するため、情報セキュリティリスクが上級経営層に確実に報告されるようにすること。

ドメイン 3 - 情報セキュリティプログラムの開発と管理

情報セキュリティ戦略と事業目標に沿った、組織の資産を識別、管理および保護する情報セキュリティプログラムを開発および維持することで、効果的なセキュリティに対する姿勢を支援する。

業務内容の申告：

- 情報セキュリティ戦略に沿った情報セキュリティプログラムを確立および／または維持すること。
- 情報セキュリティプログラムが確実に事業に付加価値を与え、また、これを維持するように、情報セキュリティプログラムと他のビジネス機能（人事[HR]、会計、調達、ITなど）が持つ業務目標と連携させること。
- 内部と外部のリソースの要件の把握、取得、および管理を行って、情報セキュリティプログラムを実行すること。
- 組織の事業目標に沿って情報セキュリティプログラムが実施されるように、情報セキュリティプロセスとリソース（人員および技術を含む）を確立し、維持すること。
- 組織の情報セキュリティの基準、ガイドライン、手順、および他の文書の確立、伝達、および維持を行って、情報セキュリティポリシーの遵守を支援し、指導すること。
- 情報セキュリティの意識向上と研修のためのプログラムを確立、推進および維持して、効果的なセキュリティ文化を醸成すること。
- 情報セキュリティ要件を組織の各種プロセス（変更コントロール、合併および買収、システム開発、事業継続、災害復旧など）に組み込んで、組織のセキュリティ戦略を維持すること。
- 情報セキュリティ要件をサードパーティ（合弁会社、委託業者、ビジネス・パートナー、顧客など）の契約と活動に組み込んで、組織のセキュリティ戦略を維持するため確立された要件の順守を監視すること。
- プログラムの管理と運用上の測定基準の確立、監視、および分析を行って、情報セキュリティプログラムの有効性と効率性を評価すること。
- セキュリティの成果について伝達するため、情報セキュリティプログラムと根底にあるビジネスプロセスの活動、傾向および全体的な有効性に関するレポートを編集し、主な利害関係者に提供すること。

ドメイン 4 - 情報セキュリティインシデントの管理

情報セキュリティインシデントの検出、調査、対応、および復旧を行う能力の計画、確立、および管理を行い、ビジネスインパクトを最小限にする。

業務内容の申告：

- 情報セキュリティのインシデントの組織的定義と重大度の序列を確立・維持して、インシデントの正確な分類とカテゴリー化を行い、インシデントに対応できるようにすること。
- インシデント対応計画を確立・維持して、情報セキュリティのインシデントに効果的かつ適時に対応できるようにすること。
- 各種プロセスを開発・実装し、ビジネスに影響を与える可能性のある情報セキュリティインシデントを適時に識別できるようにすること。
- 情報セキュリティインシデントを調査し記録するためのプロセスを確立・維持して、法令、規制、および組織の要件に準拠しながら、適切な対応と原因を特定できるようにすること。
- インシデントの通知とエスカレーションプロセスを確立・維持して、適切な利害関係者がインシデント対応管理に確実参加できるようにすること。
- 情報セキュリティインシデントに効果的に、かつ適時に対応するチームの編成、訓練および準備を行うこと。
- インシデント対応計画を定期的にテスト、評価および（該当する場合には）改訂して、情報セキュリティインシデントに効果的に対応し、対応能力を向上できるようにすること。
- コミュニケーションの計画とプロセスを確立し維持して、内部および外部の主体とのコミュニケーションを管理すること。
- 事後レビューを実施して、情報セキュリティのインシデントの根本原因を特定し、是正処置を策定し、リスクを再評価し、対応の有効性を評価し、適切な対策を実施すること。
- インシデント対応計画、災害復旧計画、および事業継続計画を統合し、維持すること。