



CERTIFIED INFORMATION SECURITY MANAGER[®]

2012 年受験者のための
CISM[®] 試験と認定ガイド

受験者のための CISM® 試験と認定ガイド

2012年度CISM試験— 日付に関する重要情報

試験日—2012年6月9日

早期締切日:	2012年2月8日
最終締切日:	2012年4月4日
試験登録の変更:	4月14日～4月20日(手数料\$50)。2012年4月20日を過ぎてからはいかなる変更も認められません。

払戻: 2012年4月13日(手数料\$100)。この日を過ぎると払戻はできません。

繰越: 2012年4月20日以前に受理された要求の場合、US \$50の手数料がかかります。2012年4月21日～5月24日に受理された要求の場合、US \$100の手数料がかかります。2012年5月24日を過ぎると、繰越は認められません。

試験日—2012年12月8日

早期締切日:	2012年8月15日
最終締切日:	2012年10月3日
試験登録の変更:	10月6日～10月12日(手数料\$50)。2012年10月12日を過ぎてからはいかなる変更も認められません。

払戻: 2012年10月5日(手数料\$100)。この日を過ぎると払戻はできません。

繰越: 2012年10月12日以前に受理された要求の場合、US \$50の手数料がかかります。2012年10月13日～11月21日に受理された要求の場合、US \$100の手数料がかかります。2012年11月21日を過ぎると、繰越は認められません。

すべての締切日の時刻は、米国イリノイ州シカゴの5p.m.(米国セントラル時間)に基づいています。

2012 受験者のための CISM® 試験と認定ガイド
本書は米国で印刷されています。

目次

はじめに.....	3
CISMプログラムがISO/IEC 17024:2003の認証を更新.....	3
CISM試験.....	3
CISM試験の受験準備.....	4
CISM試験の管理運営.....	4
CISM試験の採点.....	6
CISM試験の問題の種類.....	6
CISMの資格申請.....	6
最初のCISM資格の認定要件.....	7
CISM資格維持の要件.....	7
ISACA職業倫理規定.....	7
CISM資格の取り消し.....	7
CISMの課題と知識の記述.....	8

ISACA®とは

ISACA (www.isaca.org)は、世界160カ国95,000人をこえる会員から構成される団体で、情報システム(IS)のアシユアランスとセキュリティ、ITのエンタープライズガバナンスおよび管理、そしてIT関係のリスクやコンプライアンスにおける、知識、資格認定、コミュニティ作り、支援活動、教育機会等を、グローバルに主導しています。ISACAは独立の非営利団体として1969年に設立され、国際会議の主催、「ISACA® Journal」の刊行、国際的な情報システム監査およびコントロール基準の策定に従事しており、情報システムの信頼性と利用する価値を明らかにしています。さらに、世界的に高く評価されているCertified Information Systems Auditor® (CISA®)、Certified Information Security Manager® (CISM®)、Certified in the Governance of Enterprise IT® (CGEIT®)、そしてCertified in Risk and Information Systems Control™ (CRISC™)などの資格認定を通じ、ITスキルと知識の向上と能力の証明を行っています。ISACAはCOBIT®を継続的に更新しており、これは、特にアシユアランス、セキュリティ、リスクとコントロールの分野において、IT専門家や企業の幹部がITガバナンスと経営責任を果たし、ビジネスに価値を提供するために役立っています。

免責条項

ISACAおよびCISM認定委員会は、CISMの資格取得の指針として『2012年受験者のためのCISM®試験と認定ガイド』を策定しました。受験者が本書または他の協会の出版物を参照したことでCISM試験に合格することが保証されるものではありません。

権利の留保

Copyright © 2011 ISACA. 目的や形式を問わず、ISACAの事前の書面による許可なく、本書の内容を複製または保管することを禁じます。本書に関して、これ以外の権利ならびに許可は与えられません。全ての権利は留保されています。

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
電話: +1.847.253.1545
FAX: +1.847.253.1443
Eメール: exam@isaca.org
ウェブサイト: www.isaca.org

受験者のための CISM® 試験と認定ガイド

はじめに

公認情報セキュリティマネジャー (CISM) 資格プログラムは、経験豊富な情報セキュリティマネジャーと情報セキュリティ管理責任者のために開発されました。

CISM 資格は、企業の情報セキュリティの管理、設計および監督を行う人を対象としています。CISM 資格はセキュリティ管理が中心となりますが、セキュリティ実務に携わっている情報システムの専門家すべてに有用です。CISM 資格は国際的な慣行を促進しており、この認定資格を得た者は効果的なセキュリティ管理とコンサルティング・サービスを提供するのに必要な経験と知識を持っていることが経営トップに保証されます。CISM 資格の取得者は、セキュリティ管理のエリートネットワークの一員となり、比類のない技術を持ったプロとして世界で認められます。

CISM プログラムが ISO/IEC 17024:2003 の認証を更新

ANSI (American National Standards Institute 米国規格協会) は、CISM 認定プログラムに対して ISO/IEC 17024:2003 (人に対する認証システムを運営する団体のための一般的要件) の認証を与えています。民間非営利団体である ANSI は、製品、システム、人材認定を行う第三者組織を認可する団体です。

ISO/IEC 17024 は、特定の要件に対して個人を認定する組織が従わなければならない必要条件を指定しています。ANSI では、ISO/IEC 17024 を「資格コミュニティの世界的な標準化の促進、国間の流動性の向上、公共の安全性の強化および消費者の保護を推進するために大きな役割を担うもの」として評しています。



ANSI認定プログラム
人材認定
#0694
ISO/IEC 17024

ANSI の認定：

- ISACA の認定が提供するユニークな資格や専門性を促進する
- 認定に関する規程を保護し、法的な正当性を提供する
- 認定自体および認定資格の所有者に関して、消費者や公共の信用を高める
- 各種業界間の流動性を促進させる

ANSI による認定は、ISACA の手順が、偏見のなさ、バランス、コンセンサス、適正な手続きなどに関して、ANSI の本質的な要件を満たしていることを意味しています。この認定によって、ISACA は、CISM 資格所有者に対する優れた職業的チャンスが世界中でもたらされるものと予測しています。

CISM 試験

CISM 試験の開発 / 要領

CISM 認定委員会は試験の作成を監督し、内容が最新であることを確認します。CISM 試験の問題は、試験の品質を最大限向上させる包括的なプロセスを通じて開発されています。このプロセスでは、試験向上小委員会 (Test Enhancement Subcommittee: TES) が問題の作成者と協力して例題の作成と精査を行います。この後、例題が CISM 認定委員会に送られ、さらに審査が行われます。

実務は、試験の基本であり、CISM 資格を取得するために必要な実務経験の要件になります。この実務領域は最近更新され、2012 年 6 月の試験から実施され、そして 4 つの分野 (ドメイン) から構成されています。ドメインおよび付随する課題と知識の記述は、広範な調査と各国の当該問題の専門家によるフィードバックに基づいて作成されています。

課題と知識の記述は、CISM が実践する課題とその課題を実行するために必要な知識を表しています。受験者は、実施される課題に関連する実践的な知識に基づいてテストされます。

更新された実務領域分析のドメインおよびその割合を次に示します：

- 情報セキュリティガバナンス (24%)
- 情報リスクの管理とコンプライアンス (33%)
- 情報セキュリティプログラムの開発と管理 (25%)
- 情報セキュリティのインシデントの管理 (18%)

注：ドメインと共に記載されているパーセント数は、各ドメインから出題される質問の割合ないし重要度を示しています。各ドメインの課題と知識の記述に関する説明については、8 ~ 11 ページをご覧ください。

試験は、多肢選択方式の問題 200 問で構成されていて、6 月と 12 月の年 2 回実施されます。試験時間は 4 時間です。受験者はいくつかの言語の中から 1 つの言語を選択して試験を受けることができます。現在対応している言語のリストについては、www.isaca.org/cismterminology をご覧ください。

受験者のための CISM® 試験と認定ガイド

CISM 試験の受験準備

CISM 試験に通るために、受験者はきちんとした勉強計画を立てなければなりません。受験準備を助けるために、ISACA では教材とレビューコースを受験者にご提供しています。試験の準備に役立つ ISACA 教材については、www.isaca.org/cismguide をご覧ください。所在地や通関事情により配達に 1 週間から 4 週間を要する可能性があるため、早めにご注文ください。最新の出荷情報は www.isaca.org/shipping でご覧ください。

試験準備を進める上での学習に推奨される参考文献の総合的なリストは、2012 年 CISM レビューマニュアルでご確認いただけます。

ISACA では、共通の用語集や各資格に固有の用語集を維持しています。これらの用語集は、www.isaca.org/glossary から入手できます。

ISACA 並びに CISM 認定委員会は、これらの刊行物または他の協会の出版物およびコースが受験者の合格を保証するものではないことをおことわりしておきます。

CISM 試験の管理運営

ISACA では、国際的に認知された専門の試験代理機関を利用して、CISM 試験の作成、管理および採点をしています。

受験者が試験の管理運営について意見がある場合、試験の最後で「試験の管理運営に関するアンケート」に記入できます。試験の管理運営に関するアンケートは問題冊子の裏面にあります。アンケートの回答は解答用紙の表面の特別コードセクション（グリッド No.4）の P ~ S 欄に記入してください。

試験会場の状態または試験の内容を含む試験の管理運営に関してさらに意見または懸念事項がある場合は、書簡または電子メール (exam@isaca.org) にて ISACA 国際本部までご連絡ください。これらの意見または懸念事項は、試験日から 2 週間以内に ISACA に届くようにする必要があります。連絡する際には、受験者の ID 番号、試験会場、試験日、および特定の問題の関連情報を記入するようにしてください。試験実施後 2 週間以内に ISACA が受け取った意見のみが、試験の最終採点プロセスで考慮されます。

受験票

CISM 試験日の大体 2 ~ 3 週間前に、ISACA から受験票および電子受験票 (e-ticket) が送付されます。受験者は、Web サイト (www.isaca.org) の MyISACA ページで受験票をダウンロードすることもできます。受験票には試験日、受付時間および試験会場、当日のイベントのスケジュールと CISM 試験に持参しなければならない物が記載されています。連絡先情報を変更する場合を除き、受験者は受験票に何も記入しないことになっています。

注: 受験票を受け取るには、受験料を支払う必要があります。受験票は、記録されている現在の郵送先と電子メールアドレス宛に、ハードコピーと電子メールで送られます。受験票、および政府機関によって発行されている有効な身分証明書を持つ受験者のみに受験が許可されます。さらに、受験票の氏名が政府機関によって発行されている身分証明書の氏名と一致している必要があります。ハードコピーの受験票、または印刷した電子受験票のいずれも有効です。住所および / または電子メールアドレスが変更になった場合、ISACA のウェブサイト (www.isaca.org) でプロフィールを更新するか、exam@isaca.org にご連絡ください。

受験票に記載されている所定の受付時間および試験開始時間を必ず確認してください。試験が開始される約 30 分前に主任試験官が口頭で試験の説明を始めると、試験会場への入場はできません。口頭での試験説明が始まった後で試験場に到着した受験者は受験することができず、登録料は払い戻しできません。受験票は指定された試験会場でのみ有効です。身分証明書は試験中に確認されます。

特別措置

要求があれば、ISACA は文書による身体障害、宗教上の理由の証明のある受験者の申請に応じて受験方法に特別の措置をすることができます。こういった受験者は、試験の形式、説明方法、試験会場での飲食物、スケジュールに関して適当な変更を希望できます。試験会場での飲食物の申請が医師の注意書きと一緒に提出される以外は、**場内ではいかなる飲食も禁止されています**。特別措置を申請する場合は、2012 年 6 月の試験では 2012 年 4 月 4 日までに、2012 年 12 月の試験では 2012 年 10 月 3 日までに、関連書類を添えて書面の申請書を ISACA の国際本部に提出してください。

注記

登録は、受験票に記載されている時間に各会場で開始されます。主任試験官が口頭で試験の説明を始めたときには、すべての受験者は受付を済ませており、試験会場内にいる必要があります。試験が開始される約 30 分前に主任試験官が口頭で試験の説明を始めると、試験会場への入場はできません。

必ず受験票を持参してください。

受験票（電子受験票またはハード・コピーの受験票）は指定された試験会場でのみ有効です。有効な受験票と身分証明書 (ID) がないと試験会場には入れません。有効な身分証明書とは、受験票にあるのと同じ氏名で政府機関によって発行されている、写真付きの有効なオリジナルの身分証明書です。手書きの ID 情報は認められません。上記の条件すべてが 1 つの身分証明書に含まれていなければなりません。例としては、パスポート、運転免許証、軍隊 ID、州発行 ID、グリーンカードやナショナル ID がありますが、それらに限定されません。有効な身分証明書を持たない受験者は受験することができず、登録料金は払い戻しされません。

受験者のための CISM® 試験と認定ガイド

試験会場の規則の遵守

- 口頭での試験の説明が始まると、試験会場への入場はできません。
- 削ってある数本の HB(軟鉛)鉛筆とよく消える消しゴムを持参してください。試験会場には鉛筆と消しゴムは用意されていません。試験会場はさまざまに異なるため、各試験会場の受験環境が快適になるようあらゆる努力が払われます。受験者は各自で都合のよい着物を準備してください。
- 参考資料、白紙の用紙、メモ帳、または言語辞書を試験会場に持ち込むことはできません。
- 試験会場への電卓の持ち込みや使用はできません。
- 受験者は、いかなる種類の通信機器(携帯電話、PDA、ブラックベリー®など)も試験会場に持参してはなりません。試験実施中に受験者がこのような機器を持っていることが確認された場合、受験は無効となり、直ちに試験会場から退去するように求められます。
- 同伴者は試験会場に入れません。
- 試験会場での飲食は禁止されています (ISACA から事前の許可を得た場合は除く)。

不正行為

試験実施中に助けを与える / 受ける、メモや書類その他の資料を使用する、他の人になりすまして受験する、携帯電話を含む各種の通信機器を使用する、あるいは試験会場から試験問題、解答用紙、メモを持ち出すなどの不正行為が発覚した場合、その受験者は受験資格を失うことになり、法的措置の対象となる場合もあります。受験者が許可なく、または試験官に同伴されることなく試験室を出た場合、その受験者は試験室に戻ることはできず、受験資格を失うことになります。試験代理機関は、そのような行為について ISACA の CISM 認定委員会に報告します。

所持品に関する規定は、www.isaca.org/cismbelongings をご覧ください。ISACA も試験の代理機関も、受験者の所持品について責任を負うことはありません。

解答用紙の記入に関する注意点

- 試験開始前に、試験会場の主任試験官が口頭で解答用紙への ID 情報の記入について説明します。受験票に記載されている受験者の ID 番号などの必要な情報を正しく記入しないと、採点の遅延や間違いが発生する可能性があります。
- 各試験会場には、その地の主要言語を話せる試験官が配置されています。試験会場における主要言語以外の言語で受験することを希望しても、試験官がその言語に精通していない場合があります。ただし、書面による説明は試験の言語で記載されています。
- 受験者は問題に解答する前にすべての説明をよく読んで理解するように指示されます。指示を読み飛ばしたり、速く読みすぎたりすると、重要な情報を見逃して不合格になる恐れがあります。
- すべての解答は、解答用紙にある該当の円をマークする形式で行います。1 問で複数の解答をマークしないように注意し、適切な解答行の問題に解答していることを確認してください。解答を変更する場合、間違った解答を完全に消してから新しい解答をマークしてください。
- できる限りすべての問題に解答するようにしてください。解答を間違えてもペナルティはありません。成績は正解した問題数でのみ計算されるので、未解答の問題がないようにしてください。
- 解答し終わったら、解答用紙と問題冊子を提出してください。

試験時間の配分

- 試験は 4 時間あるので、1 問につき 1 分強の時間があります。すべての試験問題に解答できるようにペース配分することをお勧めします。そのためには、平均 50 問 / 時で解答する必要があります。
- 解答はすぐに解答用紙に記入してください。試験終了後に、問題冊子にマークした解答を解答用紙に転記する時間はありません。

適切な行為

- 試験のセキュリティ保護や得点の正当性維持のために、受験者は解答用紙に署名する必要があります。
- CISM 認定委員会には、他人を助ける / 他人から助けを受ける、メモや書類その他の資料を使用する、他の人になりすまして受験する、試験教材やメモなどを試験会場から持ち出そうとするなどの不正行為または試験規則違反が発覚した受験者を失格にする権利があります。そのような行為があった場合には、試験の代理機関から CISM 認定委員会に報告され、審査後に判断が下ることになっています。

失格または資格剥奪となる理由

- 試験会場に不正に入場する。
- 妨害行為や助けを与える / 受けるなどの行為を行う。
- 試験教材やメモなどを試験会場から持ち出そうとする。
- 他の受験者になりすまして受験する。
- 許可されていない物を試験会場に持ち込む。
- 試験実施中に受験者が通信機器(携帯電話、PDA、ブラックベリー®など)を所持している
- 受験者が許可を得ずに試験室から退去する

受験者のための CISM® 試験と認定ガイド

受験者が試験実施中に通信機器（例：携帯電話、PDA、ブラックベリー®）を所持していることが確認された場合、受験が無効となり、直ちに試験会場から退去するように求められます。

CISM 試験の採点

CISM 試験は多肢選択方式の 200 項目で構成されています。受験者の得点は段階評価スコアで通知されます。段階評価スコアは受験者の試験における実際の得点を共通の基準に変換したものです。試験に合格するには 450 点以上の得点が必要になります。例えば、段階評価スコアで満点の 800 点は、すべての問題に正解したことを表し、最低点の 200 点は、ほとんどの問題に正解できなかったことを表します。450 点は安定した水準の知識が最低限あることを示す得点で、CISM 認定委員会により設定されたものです。合格点を得た受験者は、他の要件がすべて満たされていれば、これにより資格申請が許されます。

CISM 試験には研究および分析目的でのみ含まれている問題があります。これらの問題は他の問題と区別なく出題されていますが、最終的な得点の計算には使用されません。

試験日から約 8 週間後に、正式な試験結果が受験者に郵送されます。また、受験者が出願時に同意している場合、受験者に対し、合格の可否と得点を記した電子メールが送られます。この電子メールでの通知は、結果が最初に発表された時点で受験者のプロフィールに記載されているアドレスにのみ送られます。得点の機密を確保するために、電話あるいは FAX による試験結果のお問い合わせには応じられません。電子メールでの通知がスパムフォルダに入ってしまうのを防ぐために、アドレスブック、ホワイトリスト、または安全な送信者リストに exam@isaca.org を加えておいてください。

受験者には、各ドメイン分野のサブスコアが記載されているスコア・レポートが送られます。合格者には、採点表と共に、CISM 認定の申込み方法の説明書が送られます。

サブスコアは、不合格者が試験を再受験する前にどの分野を勉強する必要があるのかわかるので有用です。不合格の受験者は、段階評価スコアの合計がサブスコアの単純平均または加重平均で計算されていないことに注意してください。

不合格の受験者は、自分の解答用紙を請求することができます。この手続きにより、マーク・ミスや複数解答や、その他コンピュータの採点を阻害する要素がなかったことを確認できます。ただし、すべての得点は通知前に複数の品質管理チェックを受けることになっており、得点の変更される可能性は低いことをご理解ください。解答用紙の得点は、試験結果が発表されてから 90 日以内に書面で認定部門に要求する必要があります。締切日を過ぎてから解答用紙の得点を要求しても処理されません。すべての請求には、受験者の名前、試験の ID 番号およびメール・アドレスが必要です。請求の際には、1 回ごとに US \$75 の費用が必要になります。

CISM 試験の問題の種類

CISM 試験の問題は、実践的な知識の評価と、一般概念および基準の応用テストを行うことを目的に開発されています。すべての問題は多肢選択形式で 1 つの最適な解答が設定されています。

CISM 試験の各問題は、ステム（問題）とオプション（解答の選択肢）で構成されています。受験者は、正しいまたは最適な解答を選択肢の中から選びます。ステムは、質問または記述の穴埋めの形式になります。場合によっては、シナリオや説明が記載されている問題が含まれていることもあります。通常、このような問題には状況の説明があり、受験者は提供されている情報に基づいて 2 つ以上の問題に解答します。受験者は各問題をよく読んでください。CISM 試験の問題では、**最もふさわしい**や**最適**などの修飾語に基づいて適切な解答を選択しなければならないこともあります。どのような場合でも、受験者は問題をよく読み、不正解だとわかっている解答を消去し、最適な選択をする必要があります。CISM 試験の問題については、www.isaca.org/cismassessment をご覧ください。

CISM の資格申請

受験者は試験に合格しただけでは、CISM 資格を取得できません。CISM 試験に合格したら、試験日から 5 年間以内に資格申請を行う必要があります。合格した受験者は、資格申請書を記入し、申請書の適切なフォームを使用して実務経験を証明する必要があります。記入済みの資格申請書の受領および承認が完了するまでは、**受験者は認定されていないため CISM の称号を使用することはできません**。認定申請が承認されなかった件に対する異議申立てのプロセスがあるため、申請に関する決定は最終的なものではないことに注意してください。認定却下に関する照会は、certification@isaca.org に送ることができます。CISM に認定されると、証明書と CISM 認定バッジが届きます。CISM のステータスを掲載、または別の方法で公表する権利（義務ではない）が ISACA にあることを申請時に承諾する必要があります。CISM の資格申請には、US \$50 の手数料が必要になります。

受験者のための CISM® 試験と認定ガイド

最初の CISM 資格の認定要件

CISM 試験に合格し、次の実務経験の要件を満たすことで、初めて資格を取得できます。

5年以上の情報セキュリティの実務経験が必要です。その内、3つ以上の実務分野で、少なくとも3年間は情報セキュリティの管理業務を経験していなければなりません。一般的な情報セキュリティの実務経験を代替することはできますが、情報セキュリティ管理の実務経験は代替できません。

実務経験の代替

他のセキュリティ資格や情報システム管理の経験は、最大で2年まで情報セキュリティ管理の実務経験として認められます。

次のいずれかを達成することで、2年間の情報セキュリティ管理の実務経験を代替できます。

- 公認情報システム監査人 (CISA) の資格保有
- 公認情報システムセキュリティプロフェッショナル (CISSP) の資格保有
- 情報セキュリティや関連分野の大学院卒（例えば、経営学、情報システムまたは情報保証）**あるいは**

次のいずれかを達成することで、1年間の情報セキュリティ管理の実務経験を代替できます。

- 満1年間の情報システム管理経験
- 満1年間の一般セキュリティ管理経験
- スキル関係のセキュリティ資格 (SANS Global Information Assurance Certification (GIAC)、Microsoft Certified Systems Engineer (MCSE)、CompTIA Security+, Disaster Recovery Institute Certified Business Continuity Professional (CBCP) または ESL IT Security Manager など)

例えば、CISA または CISSP のいずれかの資格を持つ受験者は、最大2年間の経験があるものとして認められます。しかし、受験者は4つの実務分野のうち3分野で、少なくとも3年間は情報セキュリティで管理業務を経験していなければなりません。

例外：常勤インストラクターとしての情報セキュリティ管理指導経験の2年分を、情報セキュリティ管理の実務経験の1年分として代替できます。

実務経験は、CISM の資格申請日から遡って10年以内、または試験の初回合格日から5年以内のものでなければなりません。CISM の資格申請書が、試験に合格してから5年以内に提出されない場合は、再度受験して合格することが必要となります。

CISM 試験は、実務経験の要件を満たす前に受験できます。すべての要件を満たすまでは CISM の称号は得られませんが、こういった受験は認められており、また奨励されています。

CISM 資格維持の要件

CISM 資格保有者がその資格を維持するには、次の要件を遵守する必要があります。

- 年間最低 20 CPE 時間を達成してその報告を行い、3年間の報告期間で最低でも 120 CPE 時間を達成し、詳細については、CISM 継続プロフェッショナル教育 (CPE) 指針 (www.isaca.org/cismcpepolicy) を参照してください。
- ISACA 国際本部に CPE の年間継続維持料を全額支払うこと。
- 年次の監査対象に選ばれた場合、報告した時間を立証するために CPE 活動の必要書類を記入して提出すること。
- ISACA 職業倫理規定を遵守すること。

この一般要求事項を守れない場合には、CISM の称号が取り消されます。認定書はすべて、ISACA が保有します。ある受験者が認定を受けた後、資格を取り消された場合、その者は認定書を破棄しなければなりません。

ISACA 職業倫理規定

ISACA では、協会の会員および / または当該資格保有者のプロフェッショナルまたは個人としての行動規範となる職業倫理規定を定めています。この職業倫理規定に違反すると、会員および / または資格保有者の行為が調査され、最終的に懲戒処分となる場合があります。ISACA 職業倫理規定は、www.isaca.org/ethics で確認できます。

CISM 資格の取り消し

CISM 認定委員会は、十分な検討の上で、以下のいずれかの理由から、個人の CISM 認定を取り消す権利を有します。

- CISM CPE 規則に違反した
- ISACA 職業倫理規定の条項に違反した
- 関連情報の改ざんまたは故意による隠蔽を行った
- 重要事実の虚偽表示を故意に行った
- CISM 試験または認定プロセスに関連する時期に、不誠実、不正または不適切な行為に関与したり、支援を行ったりした

受験者のための CISM® 試験と認定ガイド

CISM 実務分野の説明

CISM の課題と知識の記述

内容分野 (ドメイン)
ドメイン1—情報セキュリティガバナンス(24%)—情報セキュリティガバナンスのフレームワークと支持プロセスを確立し維持して、確実に情報セキュリティ戦略が組織の目標と目的と調和し、情報リスクが適切に管理され、プログラム・リソースが責任を持って管理されるようにする。
課題の記述
1.1 情報セキュリティ戦略を組織の目標と目的と調和するよう確立し維持して、情報セキュリティプログラムの確立と継続的管理を指導すること。
1.2 情報セキュリティガバナンスのフレームワークを確立し維持して、情報セキュリティ戦略を支援する活動を指導すること。
1.3 情報セキュリティガバナンスを企業ガバナンスに組み込んで、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確実に支援されるようにすること。
1.4 情報セキュリティ方針を確立し維持して、経営陣の指示を伝達し、基準、手順、およびガイドラインの策定を指導すること。
1.5 情報セキュリティへの投資を支援するビジネスケースを開発すること。
1.6 組織に対する内部的および外部的影響(技術、ビジネス環境、リスク許容度、所在地、法令や規制の要件など)を把握して、これらの要素が確実に情報セキュリティ戦略の対象項目になるようにすること。
1.7 経営陣上層部のコミットメントおよび利害関係者からの支援を得て、情報セキュリティ戦略の実施に成功する可能性を最大限に高めること。
1.8 情報セキュリティの役割と責任を規定し、組織全体に伝達して、明確な説明責任と権限のラインを確立すること。
1.9 測定基準(重要目標達成指標[KGI]、重要業績評価指標[KPI]、重要リスク評価指標[KRI]など)の確立、監視、評価、および報告を行って、情報セキュリティ戦略の有効性に関する正確な情報を経営陣に提供すること。
知識の記述
KS1.1 情報セキュリティ戦略を策定する方法に関する知識
KS1.2 情報セキュリティと事業の目標、目的、機能、プロセス、および実務の関係に関する知識
KS1.3 情報セキュリティガバナンスのフレームワークを実現する方法に関する知識
KS1.4 ガバナンスの基本的概念、およびそれらの概念と情報セキュリティとの関係に関する知識
KS1.5 情報セキュリティガバナンスを企業ガバナンスに組み込む方法に関する知識
KS1.6 情報セキュリティのガバナンスと戦略策定に関連して、国際的に認知された標準、フレームワーク、およびベストプラクティスに関する知識
KS1.7 情報セキュリティ方針を策定する方法に関する知識
KS1.8 ビジネスケースを開発する方法に関する知識
KS1.9 戦略的予算計画および報告方法に関する知識
KS1.10 組織に対する内部的および外部的影響(技術、ビジネス環境、リスク許容度、所在地、法令や規制の要件など)、およびこれらが情報セキュリティ戦略に影響を及ぼす方法に関する知識
KS1.11 情報セキュリティについて経営陣上層部のコミットメントおよび利害関係者からの支援を得る方法に関する知識
KS1.12 情報セキュリティ管理の役割と責任に関する知識
KS1.13 組織構造と権限のラインに関する知識
KS1.14 報告と伝達の経路を組織全体に新規に確立するか既存の経路を活用する方法に関する知識
KS1.15 測定基準(重要目標達成指標[KGI]、重要業績評価指標[KPI]、重要リスク評価指標[KRI]など)の選択、実施、および解釈を行う方法に関する知識
ドメイン2—情報リスクの管理とコンプライアンス(33%)—情報リスクを許容できるレベルまで管理して、組織の事業要件とコンプライアンス要件を満たす。
課題の記述
2.1 情報資産のランク付けのプロセスを確立し維持して、資産保護の手段が事業価値に確実に比例するようにすること。
2.2 法令、規制、組織、およびその他の該当する要件を把握して、不遵守のリスクを許容できるレベルまで管理すること。

受験者のための CISM® 試験と認定ガイド


内容分野 (ドメイン)
ドメイン2—情報リスクの管理とコンプライアンス(続き)
2.3 リスク評価、脆弱性評価、および脅威分析が確実に定期的かつ一貫して実行されて、組織の情報に対するリスクを把握できるようにすること。
2.4 適切なリスク対応オプションを判断して、リスクを許容できるレベルまで管理すること。
2.5 情報セキュリティコントロールを評価して、それらが適切でありリスクを許容できるレベルにまで効果的に低減するかどうかを判断すること。
2.6 現在のリスクレベルと目標レベルとのギャップを把握して、リスクを許容できるレベルまで管理すること。
2.7 情報リスク管理を事業とITの各プロセス(開発、調達、プロジェクト管理、合併・買収など)に組み込んで、一貫性があり包括的な情報リスク管理プロセスを組織全体に推進すること。
2.8 既存のリスクを監視して、変化を確実に把握し適切に管理すること。
2.9 情報リスクにおける不遵守やその他の変化について該当する経営陣に報告して、リスク管理の意思決定プロセスを支援すること。
知識の記述
KS2.1 事業目的に一致する情報資産のランク付けモデルを確立するための方法に関する知識
KS2.2 情報の資産とリスクの責任と所有権を割り当てるために使用される方法に関する知識
KS2.3 有害な事象がビジネスに及ぼす影響を評価するための方法に関する知識
KS2.4 情報資産の評価方法に関する知識
KS2.5 情報セキュリティに関連する法令、規制、組織、およびその他の要件に関する知識
KS2.6 新たな情報セキュリティ上の脅威と脆弱性に関する、評判が良く、信頼できる時宜になつた情報源に関する知識
KS2.7 リスクの再評価および情報セキュリティ・プログラム要素の変更が必要になる可能性のある事象に関する知識
KS2.8 情報の脅威、脆弱性、および発現度とそれらの進展性に関する知識
KS2.9 リスクの評価と分析の方法論に関する知識
KS2.10 リスクの優先度設定に使用される方法に関する知識
KS2.11 リスクの報告要件(頻度、対象読者、項目など)に関する知識
KS2.12 リスクの監視に使用される方法に関する知識
KS2.13 リスク対応戦略とその適用方法に関する知識
KS2.14 コントロール・ベースラインモデリング、およびリスクを基準とする評価と同モデリングとの関係に関する知識
KS2.15 情報セキュリティのコントロールと対策、およびそれらの有効性と効率の分析方法に関する知識
KS2.16 情報セキュリティに関連するギャップ分析法に関する知識
KS2.17 リスク管理を事業とITプロセスに組み込むための手法に関する知識
KS2.18 コンプライアンス報告のプロセスと要件に関する知識
KS2.19 リスク対応オプションを評価するための費用対効果分析に関する知識
ドメイン3—情報セキュリティプログラムの開発と管理(25%)—情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し管理する。
課題の記述
3.1 情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し維持すること。
3.2 情報セキュリティプログラムとその他のビジネス機能(人事[HR]、経理、調達、ITなど)との間で整合性を確実に取って、ビジネスプロセスへの組み込みを支援すること。
3.3 内部と外部のリソースの要件の把握、取得、管理、および定義を行って、情報セキュリティプログラムを実行すること。
3.4 情報セキュリティアーキテクチャ(人材、プロセス、技術)を確立し維持して、情報セキュリティプログラムを実行すること。
3.5 組織の情報セキュリティの基準、手順、ガイドライン、および他の文書の確立、伝達、および維持を行って、情報セキュリティ方針の遵守を支援し指導すること。
3.6 情報セキュリティの周知と研修のためのプログラムを確立し維持して、セキュリティで保護された環境と効果的なセキュリティ文化を推進すること。

受験者のための CISM® 試験と認定ガイド

内容分野 (ドメイン)
ドメイン3—情報セキュリティプログラムの開発と管理(続き)
3.7 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、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ベースラインを維持すること。
3.8 情報セキュリティ要件をサードパーティ(合併会社、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ベースラインを維持すること。
3.9 プログラムの管理と運用上の測定基準の確立、監視、および定期的な報告を行って、情報セキュリティプログラムの有効性と効率を評価すること。
知識の記述
KS3.1 情報セキュリティプログラムの要件と他のビジネス機能の要件を合致させる方法に関する知識
KS3.2 内部と外部のリソースの要件の把握、取得、管理、および定義を行うための方法に関する知識
KS3.3 情報セキュリティ技術、最近の動向(クラウドコンピューティング、モバイルコンピューティングなど)、および根底にある概念に関する知識
KS3.4 情報セキュリティコントロールを設計する方法に関する知識
KS3.5 情報セキュリティアーキテクチャー(人材、プロセス、技術)およびそれらを適用する方法に関する知識
KS3.6 情報セキュリティの基準、手順、およびガイドラインを策定する方法に関する知識
KS3.7 情報セキュリティの方針、基準、手順、およびガイドラインを実施し伝達する方法に関する知識
KS3.8 効果的な情報セキュリティの周知と研修のプログラムを確立し維持するための方法に関する知識
KS3.9 情報セキュリティ要件を組織の各種プロセスに組み込む方法に関する知識
KS3.10 情報セキュリティ要件を契約およびサードパーティ管理プロセスに組み込むための方法に関する知識
KS3.11 情報セキュリティの運用上の測定基準の設計、実施、および報告を行うための方法に関する知識
KS3.12 情報セキュリティコントロールの有効性および適用性をテストする方法に関する知識
ドメイン4—情報セキュリティのインシデントの管理(18%)—情報セキュリティのインシデントの検知、調査、対応、および復旧を行う能力の計画、確立、および管理を行って、ビジネスへの影響を最小限にとどめる。
課題の記述
4.1 情報セキュリティのインシデントの組織内定義と重大度の序列を確立し維持して、インシデントを正確に把握し対応できるようにすること。
4.2 インシデント対応計画を確立し維持して、情報セキュリティのインシデントに効果的かつ即座に対応できるようにすること。
4.3 各種プロセスを開発し実施して、情報セキュリティのインシデントを即座に把握できるようにすること。
4.4 情報セキュリティのインシデントを調査し記録するためのプロセスを確立し維持して、法令、規制、および組織の要件に準拠しながら、適切に対応し原因を究明できるようにすること。
4.5 インシデントのエスカレーションと通知のプロセスを確立し維持して、該当する利害関係者がインシデント対応管理に確実に参加できるようにすること。
4.6 情報セキュリティインシデントに即座に効果的に対応するチームの編成、訓練、および準備を行うこと。
4.7 インシデント対応計画を定期的にテストし見直して、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。
4.8 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。
4.9 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。
4.10 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の間の統合を確立し維持すること。
知識の記述
KS4.1 インシデント対応計画の要素に関する知識
KS4.2 インシデント管理の概念と実務に関する知識
KS4.3 事業継続性計画(BCP)と災害復旧計画(DRP)、およびそれらとインシデント対応計画との関係に関する知識
KS4.4 インシデント分類法に関する知識
KS4.5 損害抑制法に関する知識
KS4.6 通知とエスカレーションのプロセスに関する知識

受験者のための CISM® 試験と認定ガイド

内容分野 (ドメイン)
KS4.7 情報セキュリティインシデントの特定および管理における役割と責任に関する知識
KS4.8 インシデント対応チームで十分に備えておく必要があるツールや機器の種類または供給源に関する知識
ドメイン4—情報セキュリティのインシデントの管理 (続き)
KS4.9 証拠の収集、保存、および提出のためのフォレンジックの要件と能力(証拠の許容性、品質、完全性、分析過程の管理など)に関する知識
KS4.10 内部と外部のインシデント報告の要件と手順に関する知識
KS4.11 根本原因の特定と是正処置の決定を行うための事後レビュー実務および調査方法に関する知識
KS4.12 情報セキュリティインシデントによって生じる損害、費用、および他のビジネスへの影響を定量化する技術に関する知識
KS4.13 情報セキュリティイベントの検知、ログ作成、および分析を行う技術とプロセスに関する知識
KS4.14 情報セキュリティのインシデントの調査に使用できる内部と外部のリソースに関する知識



2012 年度 CISM 試験の準備をしよう

2012 年度公認情報セキュリティマネージャー (CISM) 試験の準備と職業能力の開発のためのレビュー資料

Certified Information Security Manager® (CISM®) 試験に合格するには、学習計画を立案すべきです。受験者が学習計画をうまく立案することができるように、情報システムコントロール協会は、学習のための資料とレビューコースを提供しています。以下のものが含まれます。

学習のための教材

- CISM® *Review Manual 2012*
- 2012 年 CISM® 試験サンプル問題& 解答・解説集
- 2012 年 CISM® 試験サンプル問題& 解答・解説集(追補版)
- CISM® Practice Question Database v12

ご注文は www.isaca.org/cismbooks にて承ります。

レビューコース

- 支部主催レビューコース

お住まいの地域のレビューコースを検索又は受講される場合は、www.isaca.org/cismreview にアクセスしてください。