情報システム監査および保証業務基準
1202 計画におけるリスク評価

情報システム監査および保証業務の専門性およびそのような業務を実施するために必要なスキルには、情報システム監査および保証業務に専ら適用される基準が必要となる。情報システム監査および保証業務基準の策定と普及は、ISACA®の職業的専門家による監査業界に対する貢献の基礎となる。

情報システム監査および保証業務基準は、情報システム監査と監査報告の必須要件を規定し、以下の情報を提供する。

- 情報システム監査および保証業務の専門家に対し、ISACA 職業倫理規定（ISACA Code of Professional Ethics）に規定された職業的専門家の責任を果たすために必要な、最低限許容可能な実施水準
- 経営者およびその他の関係者からの、業務実施者の作業に関する職業的専門家のへの期待
- CISA®（Certified Information Systems Auditor®）資格保有者に対し、その要件。この基準に違反すると、ISACA 理事会または関係する委員会により CISA 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る。

情報システム監査および保証業務の専門家は、業務が ISACA 情報システム監査および保証業務基準またはその他の適用される職業的専門家としての基準に従って実施されたという表明文を、必要に応じて各自の作業において含めるべきである。

情報システム監査および保証業務の専門家のための *ITAF™* フレームワークは、以下の複数レベルのガイダンスを提供している。

- **基準**は、次の 3 つに分類される。
  - 一般基準（1000 シリーズ） – 情報システム監査および保証業務の専門家が活動するガイダンスとなる原則。これはすべての業務の実施に適用され、情報システム監査および保証業務の専門家の倫理、独立性、客観性および正当な注意、ならびに知識、能力およびスキルに関するものである。「基準」の記述（太字表記）は必須事項である。
  - 実施基準（1200 シリーズ） – 計画と監督、範囲の決定、リスクと重要性、資源の動員、監督と業務割り当ての管理、監査および保証業務の証拠、職業的専門家としての判断と正当な注意等、業務の実施に関するものである。
  - 報告基準（1400 シリーズ） – 報告書の種類、伝達手段および伝達される情報に関するものである。
- **ガイドライン**は、基準を支援するものであり、同様に 3 つに分類される。
  - 一般ガイドライン（2000 シリーズ）
  - 実施ガイドライン（2200 シリーズ）
  - 報告ガイドライン（2400 シリーズ）
- **ツールと技法**は、情報システム監査および保証業務の専門家のための追加的ガイダンス、例えばホワイトペーパー、情報システム監査・保証業務手続書、COBIT® 5 製品シリーズ、を提供する。

ITAF で使用する用語のオンライン用語集が *www.isaca.org/glossary* で提供されている。

免責条項：ISACA は、ISACA の職業倫理規定（ISACA Code of Professional Ethics）に規定された職業的専門家の責任を果たすために必要な最低限許容可能な実施水準として、当ガイダンスを策定した。ISACA は当文書の利用が成功する結果を保証するとは主張していない。当出版物は、適切な手続やテストをすべて含むものではなく、また同じ結果を得るための他の手続やテストを排除するものではない。個別の手続やテストの妥当性を判断する際、統制の専門家は、特定のシステムや情報システム環境から生じる特定の統制の状況に対し、自らの職業的専門家としての判断を適用すべきである。

ISACA の Carrier Management Committee (PSCMC)は、基準およびガイダンスの策定に際して広範な意見聴取に取り組んでいる。ドキュメントの発行に先立ち、パブリックコメントを得るため国際的に公開草案を公表する。コメントは、E メール（*standards@isaca.org*）、ファクス（+1.847.253.1443）または郵送（ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA）で、Director of Professional Standards Development 宛に提出できる。

情報システム監査および保証業務基準 1202 計画におけるリスク評価

基準

1202.1 **情報システム監査および保証業務機能は、適切なリスク評価のアプローチおよび支援する手法を用いて、基本的な情報システム監査計画を作成し、情報システム監査資源の効果的な配分に関する優先順位を決定すること。**

1202.2 **情報システム監査および保証業務の専門家は、個々の監査業務の計画時、レビュー対象になっている領域に関連するリスクを識別し、評価を実施すること。**

1202.3 **情報システム監査および保証業務の専門家は、事業体への主題リスク、監査リスクおよび関連するリスクの発現可能性について検討すること。**

重要事項

進行中の活動の計画時、情報システム監査および保証業務機能は、以下を満たすべきである。

- 情報システム監査計画の作成を円滑にするため、少なくとも年次でリスクを実施して文書化する。
- リスク評価の一部として、組織の戦略的計画および目的、ならびに事業体のリスク管理の枠組みと取り組みを含める。
- 各々の情報システム監査および保証業務に関して、業務要件を満たすために必要な情報システム監査資源の定量化および正当化を行う。
- 監査対象の領域や項目を選択する際に、また特定の情報システム監査および保証業務を立案し、実施する決定をする際に、リスク評価を利用する。
- 監査の利害関係者およびその他の適切な関係者から、リスク評価の承認を求める。
- 情報システム監査および保証業務の作業について、リスクの評価に基いて優先順位を付け、スケジュールする。
- リスク評価に基づき、次のような計画を策定する。
  - 情報システム監査および保証業務活動のフレームワークとして機能する
  - 情報システム以外の監査および保証業務の要求事項と活動を考慮する
  - 最低年次で更新し、ガバナンス責任者の承認を得る
  - 監査規程に規定されている責任に対応する

個々の監査業務の計画時、情報システム監査および保証業務の専門家は、以下を満たすべきである。

- レビュー対象の領域に関するリスクを識別し、評価を実施する。
- 各々の監査業務に際し、レビュー対象の領域に関連するリスクの事前評価を実施する。個別の監査業務の目的は、リスクの事前評価の結果を反映すべきである。
- リスク領域を検討し、特定の監査業務を計画する際に、是正活動を含め、以前の監査、レビューおよび発見事項を検討する。また、取締役会による包括的なリスク評価プロセスについても検討する。
- 情報システム監査を計画、実施する際には、監査リスクを許容可能な水準まで軽減することを試み、情報システムの主題および関連する統制の適切な評価により監査の目的を満たす。

情報システム監査および保証業務基準 1202 計画におけるリスク評価

- 特定の情報システム監査手続を計画する際には、重要性の許容値が低いほど、監査の期待精度が高まり、監査リスクが高くなることを認識する。
- 重要性が高いリスクを低減するため、追加的な保証を得るべく運用評価手続を拡大する（統制リスクを低減する）か、実証を拡大する（発見リスクを低減する）かの両方またはいずれか一方により補完する。

用語

用語	定義
監査規程	内部監査アクティビティの目的、権限および責任を規定するガバナンス責任者に承認された文書。 監査規程は以下を満たすべきである。 • 事業体における内部監査機能の位置付けを確立する • 情報システム監査および保証業務の実施に関連する、記録、担当者および有形資産へのアクセスを許可する • 監査機能の活動範囲を規定する
監査リスク	監査の発見事項に基づいて誤った結論に到達するリスク。監査リスクの 3 つの要素は以下のとおり。 • 統制リスク • 発見リスク • 固有リスク
監査主題リスク	レビュー対象の領域に関する以下のリスク • 事業上のリスク（顧客への支払い能力、信用力、市場要素等） • 契約リスク（債務、価格、種類、罰則等） • カントリーリスク（政治、環境、安全等） • プロジェクトリスク（資源、スキルセット、手法、製品安定性等） • 技術リスク（ソリューション、アーキテクチャ、ハードウェアとソフトウェアのインフラストラクチャネットワーク、配信チャネル等） 固有リスクを参照。
統制リスク	内部統制システムによって適時に防止または発見することができない重要な誤謬が存在するリスク。 （固有リスクを参照。）
発見リスク	情報システム監査および保証業務の専門家の実証手続では、単独でまたは他の誤謬との組合せで重要となる誤謬を発見できないリスク。監査リスクを参照。
固有リスク	経営者が実施済みか講じるであろう措置（例：統制の導入）を考慮に入れない場合のリスクの水準またはリスクの発現可能性。統制リスクを参照。
重要性	監査対象の主体の機能に与える影響に関する情報の重要性に関わる監査上の概念。事業体全体における、特定の事項の相対的な重大性または重要性の表現。
リスク評価	リスクとその潜在的な影響を識別し、評価するために使用されるプロセス。

	リスク評価は、情報システムの年次監査計画に含めるために、事業体の最大のリスク、脆弱性またはそれらの発現可能性を示す項目または領域を識別する際に使用される。 リスク評価は、プロジェクトデリバリーおよびプロジェクト効果に関わるリスクの管理にも使用する。
実証手続	監査期間中の活動や取引の網羅性、正確性、実在性について監査証拠を得ること。

ガイドラインへのリンク

種類	表題
ガイドライン	2202 計画におけるリスク評価

適用開始日　本 ISACA 基準は、2013 年 11 月 1 日以降に開始されるすべての情報システム監査および保証業務に適用される。