



情報システム監査および保証業務基準 1001 監査規程

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・保証業務手順書、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。

ISACA 2012-2013 Professional Standards and Career Management Committee	
Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
坂川 克己, CISA, CRISC, PMP	株式会社 JIEC, Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

情報システム監査および保証業務基準 1001 監査規程

基準

- 1001.1** 情報システム監査および保証業務機能は、監査規程に監査機能を適切に文書化し、目的、実行責任者、権限者および説明責任を示すこと。
- 1001.2** 情報システム監査および保証業務機能は、事業体内の適切なレベルで監査規程の合意および承認を得ること。

重要事項

- 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。
- 以下の点について、伝達できる詳細さで、情報システム内部監査および保証業務機能の活動を定義した監査規程を作成する。
 - 情報システム監査および保証業務機能の権限、目的、責任および制約
 - 情報システム監査および保証業務機能の独立性および説明責任
 - 情報システム監査業務または保証業務実施中の被監査組織の役割と責任
 - 情報システム監査および保証業務の専門家が情報システム監査および保証業務の実施において従う職業的専門家としての基準
 - 監査規程について、少なくとも年1回、また責任が変更された場合にはより頻繁にレビューを行う。
 - 目的および責任が適切に文書化され、かつ維持されていることを確実にするため、必要に応じて監査規程を更新する。
 - 情報システム監査または保証業務ごとに、監査規程を正式に被監査組織に伝達する。

用語

用語	定義
保証業務	事業体向けに、リスク管理、統制またはガバナンスプロセスの評価を提供するための、証拠の客観的な検討。 範囲に関する注記：例として、財務、成果、コンプライアンスおよびシステムのセキュリティ業務が挙げられる。
監査規程	内部監査活動の目的、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。 <ul style="list-style-type: none"> • 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
監査業務	監査、コントロールセルフアセスメントのレビュー、不正の検討または相談といった、特定の監査の割り当て、職務またはレビュー活動。 監査業務には、関連する特定の目的を達成するために策定された複数の職務または活動が含まれることがある。
独立性	客観性または外観的な客観性を脅威にさらすような状態からの解放。かかる客観性に対する脅威は、個々の監査人、業務、機能、組織のレベルで管理されなければならない。

情報システム監査および保証業務基準 1001 監査規程

	独立性には、精神的独立性および外観的独立性が含まれる。
--	-----------------------------

ガイドラインへのリンク

種類	表題
ガイドライン	2001 監査規程

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。