

Le caractère spécialisé de l'audit et de l'assurance des systèmes d'information (SI) et les compétences requises pour effectuer ces missions rendent nécessaire la mise en œuvre de normes qui s'appliquent spécifiquement à ces disciplines. Le développement et la promulgation de normes d'audit et d'assurance des SI sont des pierres angulaires de la contribution de l'ISACA[®] à la communauté des auditeurs.

Les normes d'audit et d'assurance des systèmes d'information (SI) définissent les obligations en matière d'audit et de rapports et informent :

- Les professionnels de l'audit et de l'assurance des SI sur le niveau minimum de performances requis pour satisfaire aux responsabilités stipulées dans le Code d'éthique professionnelle de l'ISACA
- Les dirigeants d'entreprise et les autres parties intéressées sur les attentes de la profession concernant le travail des praticiens
- Les titulaires de la certification CISA[®] (Certified Information Systems Auditor[®] – Auditeur informatique certifié) sur les exigences de leur charge. Toute incapacité à mettre en œuvre ces normes peut entraîner une enquête sur la conduite du titulaire de la certification CISA par le Conseil d'administration de l'ISACA ou tout autre Comité approprié et, en définitive, des actions disciplinaires.

Les professionnels de l'audit et de l'assurance des SI doivent indiquer dans leur travail, si cela se justifie, que la mission a été exécutée conformément aux normes d'audit et d'assurance SI de l'ISACA ou à d'autres normes professionnelles applicables.

La structure *ITAF*[™] à l'intention des professionnels de l'audit et de l'assurance des SI fournit de nombreux niveaux d'assistance :

- **Normes**, divisées en trois catégories :
 - Normes générales (série 1000) – Ce sont les principes directeurs selon lesquels fonctionne la profession de l'audit et de l'assurance des SI. Elles s'appliquent à la conduite de toutes les missions et traite de l'éthique, de l'indépendance, de l'objectivité et de l'obligation de diligence des professionnels de l'audit et de l'assurance des SI, ainsi que de leurs connaissances, compétences et expertises. Les déclarations de normes (en **caractères gras**) sont obligatoires.
 - Normes de performance (série 1200) – Elles traitent de la conduite de la mission, notamment de la planification et de la supervision, de la définition du périmètre, du risque et de la matérialité, de la mobilisation des ressources, de la gestion de la supervision et de la mission, des preuves en matière d'audit et d'assurance et de l'exercice du jugement professionnel et de la diligence nécessaire
 - Normes de reporting (série 1400) – Elles traitent des types de rapports, des moyens de communication et des informations communiquées
- **Directives**, qui appuient les normes, également divisées en trois catégories :
 - Directives générales (série 2000)
 - Directives relatives à l'exécution (série 2200)
 - Directives relatives au reporting (série 2400)
- **Outils et techniques**, qui fournissent des informations supplémentaires à l'intention des professionnels de l'audit et de l'assurance des SI, par exemple : livres blancs, programmes d'audit et d'assurance des SI, la famille de produits COBIT[®] 5

Un glossaire en ligne des termes utilisés dans l'ITAF est disponible à la page www.isaca.org/glossary.

Exclusion de responsabilité : L'ISACA a conçu ces directives comme le niveau minimum de performances requis pour satisfaire aux responsabilités stipulées dans son Code d'éthique professionnelle. L'ISACA ne saurait garantir que l'utilisation de ce produit constitue une assurance de résultat. La présente publication ne saurait être considérée comme incluant l'ensemble des procédures et tests adaptés ou comme excluant d'autres procédures et tests susceptibles de conduire raisonnablement à des résultats similaires. Pour déterminer si une procédure ou un test spécifique est approprié, les professionnels du contrôle doivent en tant que professionnels se faire leur propre opinion en fonction des cas particuliers de contrôle rencontrés dans leurs systèmes ou environnement SI spécifique.

Le Comité ISACA de gestion des normes et carrières professionnelles (PSCMC, Professional Standards and Career Management Committee) s'engage à consulter largement dans le cadre de la préparation des normes et directives. Avant d'éditer ses documents, il publie des projets de documents à l'échelle internationale pour recueillir les avis du grand public. Les avis peuvent aussi être portés à l'attention du directeur du développement des normes professionnelles par courriel à standards@isaca.org, fax (+1.847. 253.1443) ou par courrier postal (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

ISACA 2012-2013 Professional Standards and Career Management Committee

Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, États-Unis
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, Royaume-Uni
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, États-Unis
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaisie
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, Nouvelle-Zélande
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japon
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgique
Timothy Smith, CISA, CISSP, CPA	LPL Financial, États-Unis
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentine

Norme d'audit et d'assurance des SI 1207 - Irrégularités et actes illégaux

Déclarations

- 1207.1** Les professionnels de l'audit et de l'assurance des SI doivent considérer le risque d'irrégularités et d'actes illégaux pendant la mission.
- 1207.2** Les professionnels de l'audit et de l'assurance des SI doivent conserver une attitude de scepticisme professionnel pendant la mission.
- 1207.3** Les professionnels de l'audit et de l'assurance des SI doivent documenter et communiquer toute irrégularité matérielle ou acte illégal à la partie concernée dans les meilleurs délais.
-

Principaux aspects

Les professionnels de l'audit et de l'assurance des SI doivent :

- Réduire le risque d'audit à un niveau acceptable lors de la planification et de l'exécution de l'engagement :
 - En étant conscients du fait que les erreurs matérielles, les déficiences des contrôles ou les anomalies dues à des irrégularités et des actes illégaux peuvent exister, indépendamment de l'évaluation du risque d'irrégularités et d'actes illégaux
 - En acquérant une bonne compréhension de l'entreprise et de son environnement, y compris des contrôles internes destinés à empêcher ou détecter des irrégularités et actes illégaux pertinents pour l'objet, la portée et les objectifs de la mission
 - En collectant des éléments probants suffisants et pertinents pour déterminer si la direction ou d'autres personnes dans l'entreprise ont connaissance d'irrégularités ou d'actes illégaux avérés, suspectés ou allégués
- Étudier les relations inhabituelles ou inattendues susceptibles d'indiquer un risque d'erreur matérielle, de déficience des contrôles ou d'anomalie dus à des irrégularités et actes illégaux lors de l'exécution des procédures d'audit,
- Concevoir et exécuter des procédures destinées à tester le caractère approprié des contrôles internes et le risque de contournement par la direction de contrôles destinés à prévenir ou détecter des irrégularités et actes illégaux,
- Évaluer si les erreurs, déficiences des contrôles ou anomalies identifiées peuvent être indicatives d'une Irrégularité ou d'un acte illégal. Si tel est le cas, envisager les implications dans d'autres aspects de la mission, en particulier dans les déclarations de la direction.
- Obtenir des déclarations annuelles écrites de la direction, ou plus souvent selon la mission, comportant :
 - La reconnaissance de la responsabilité de la direction dans l'élaboration et la mise en œuvre de contrôles internes visant à prévenir et à repérer les irrégularités ou les actes illégaux.
 - La divulgation des résultats pertinents de toute évaluation des risques indiquant que des erreurs, des déficiences du contrôle ou des anomalies peuvent exister par suite d'une irrégularité ou d'un acte illégal.
 - La divulgation de la connaissance par la direction d'irrégularités et d'actes illégaux affectant l'entreprise en relation avec la direction et les employés ayant des rôles importants dans le contrôle interne.
 - La divulgation de la connaissance par la direction de tout soupçon d'irrégularité et d'acte illégal affectant l'entreprise, tels que communiqués par des employés, anciens employés, organismes de réglementation et autres.

Norme d'audit et d'assurance des SI 1207 - Irrégularités et actes illégaux

Principaux aspects
(suite)

- Communiquer ponctuellement :
 - Au niveau de direction approprié toute information identifiée ou obtenue selon laquelle une irrégularité ou un acte illégal important peut exister
 - Aux personnes chargées de la gouvernance toute irrégularité et tout acte illégal importants impliquant la direction ou des employés qui ont des rôles importants en matière de contrôle interne
- Signaler aux personnes chargées de la gouvernance toute faiblesse matérielle de la conception et de la mise en œuvre des contrôles internes destinée à prévenir et détecter toute irrégularité et tout acte illégal identifiés pendant la mission, même s'ils sont extérieurs au périmètre.
- Envisager les exigences juridiques et professionnelles applicables à la présentation de rapports eu égard aux circonstances.
- Envisager leur retrait de la mission si des erreurs, déficiences de contrôles, anomalies ou actes illégaux importants affectent la poursuite de l'exécution de la mission.
- Documenter l'ensemble des communications, planifications, résultats, évaluations et conclusions liés aux irrégularités matérielles et aux actes illégaux signalés à la direction, aux personnes chargées de la gouvernance, aux autorités de réglementation et autres.

Terminologie

Terme	Définition
Irrégularité	Violation d'une politique établie de la direction ou d'une exigence réglementaire. Il peut s'agir d'anomalies ou d'omissions délibérées d'informations concernant le domaine audité ou l'entreprise dans son ensemble, d'une négligence grave ou d'actes illégaux non intentionnels.
Anomalie significative	Une déclaration inexacte, accidentelle ou intentionnelle, qui affecte les résultats d'un audit d'une manière mesurable
Scepticisme professionnel	Une attitude comprenant un esprit curieux et une évaluation critique des éléments probants de l'audit. Source : American Institute of Certified Public Accountants (AICPA) AU 230.07

Liens vers les normes et directives

Type	Titre
Norme	1008 Critères
Norme	1202 Évaluation du risque dans la planification
Norme	1205 Éléments probants
Directive	2206 Utilisation du travail d'autres experts
Directive	2207 Irrégularités et actes illégaux

Date de prise d'effet

La présente norme ISACA s'appliquera à toutes les missions d'audit et d'assurance des SI débutant à compter du 1^{er} novembre 2013.