Norme d'audit et d'assurance des SI 1401 - Rapports

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).

Norme d'audit et d'assurance des SI 1401 - Rapports

Déclarations

1401.1 Les professionnels de l'audit et de l'assurance des SI doivent fournir un rapport afin de communiquer les résultats à l'achèvement de la mission, comprenant :

- **Identification de l'entreprise, de ses destinataires pressentis et de toute restriction relative à son contenu et sa diffusion**
- **La portée, les objectifs de la mission, la période couverte et la nature, le calendrier et l'étendue des travaux exécutés**
- **Les résultats, conclusions et recommandations**
- **Toute restriction ou limitation de la portée signalée par le professionnel de l'audit et de l'assurance des SI concernant la mission**
- **La signature, la date et la diffusion conformément aux termes de la charte d'audit ou de la lettre de mission**

1401.2 Les professionnels de l'audit et de l'assurance des SI doivent veiller à ce que les conclusions du rapport d'audit soient étayées par des éléments probants suffisants et appropriés.

Principaux aspects

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

- Obtenir des déclarations écrites pertinentes de l'entité auditée indiquant en détails clairs les domaines de la mission, les problèmes survenus et leur résolution, ainsi que les affirmations faites par l'entité auditée
- Déterminer que les déclarations de l'entité auditée ont été signées et datées par celle-ci de manière à indiquer qu'elle reconnaît ses responsabilités dans le cadre de la mission
- Documenter et conserver dans les documents de travail toute déclaration reçue pendant le déroulement de la mission, que ce soit par écrit ou oralement. Dans le cas des missions d'attestation, les déclarations de l'entité auditée doivent être obtenues par écrit pour réduire les éventuels malentendus.
- Adapter la forme et le contenu du rapport au type de mission exécutée, telle que :
  - Audit (direct ou attestation)
  - Contrôle (direct ou attestation)
  - Procédures convenues
- Décrire dans le rapport les faiblesses matérielles ou importantes et leur incidence sur la réalisation des objectifs de la mission.
- Discuter du contenu du projet de rapport avec la direction du domaine objet de la mission avant sa finalisation et sa diffusion et intégrer les réactions de la direction aux résultats, conclusions et recommandations du rapport définitif, le cas échéant.
- Communiquer les déficiences importantes et faiblesses matérielles de l'environnement de contrôle aux personnes chargées de la gouvernance et, le cas échéant, à l'autorité responsable, et signaler dans le rapport que ces éléments ont été communiqués.
- Faire référence à tout rapport distinct dans le rapport final.
- Communiquer à la direction de l'entité auditée les insuffisances de contrôle interne qui, sans être négligeables, ne sont pas substantielles. Dans ces cas, les personnes chargées de la gouvernance ou l'autorité responsable doivent être informées de la communication à la direction de l'entité auditée de ces déficiences du contrôle interne.

- Identifier les normes appliquées à la conduite de la mission et communiquer toute non-conformité avec ces normes, le cas échéant.

Terminologie

Terme	Définition
Informations pertinentes	En ce qui concerne les contrôles, donne à l'évaluateur des indications significatives sur le fonctionnement des contrôles sous-jacents ou de la composante de contrôle. Les informations qui confirment directement le fonctionnement des contrôles sont les plus pertinentes. Les informations qui se rapportent indirectement au fonctionnement des contrôles peuvent aussi être pertinentes, mais moins que les informations directes. Se reporter aux objectifs de qualité des informations COBIT 5
Informations fiables	Informations exactes, vérifiables et provenant d'une source objective. Se reporter aux objectifs de qualité des informations COBIT 5
Informations suffisantes	Des informations sont suffisantes lorsque les évaluateurs en ont réuni suffisamment pour parvenir à une conclusion raisonnable. Pour que des informations soient suffisantes, elles doivent toutefois être d'abord adéquates. Se reporter aux objectifs de qualité des informations COBIT 5
Informations adéquates	Informations pertinentes (correspondant à leur objet prévu), fiables (exactes, vérifiables et provenant d'une source objective) et ponctuelles (produites et utilisées dans un cadre temporel approprié). Se reporter aux objectifs de qualité des informations COBIT 5
Informations ponctuelles	Informations produites et utilisées dans un cadre temporel rendant possible la prévention ou la détection de déficiences des contrôles avant qu'elles ne deviennent matérielles pour l'entreprise. Se reporter aux objectifs de qualité des informations COBIT 5

Liens vers les normes et directives

Type	Titre
Directive	2401 Rapports

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 1er novembre 2013.