Norme d'audit et d'assurance des SI 1202 — Évaluation du risque dans la planification

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 1202 - Évaluation du risque dans la planification

Déclarations

1202.1 La fonction d’audit et d’assurance des SI doit utiliser une approche d’évaluation du risque et une méthodologie à l’appui appropriées pour élaborer le plan général d’audit des SI et définir les priorités en vue d’une allocation efficace des ressources d’audit des SI.

1202.2 Les professionnels de l’audit et de l’assurance des SI doivent identifier et évaluer les risques pertinents eu égard au domaine examiné lors de la planification de chaque mission.

1202.3 Les professionnels de l’audit et de l’assurance des SI doivent prendre en considération le risque lié à l’objet, le risque d’audit et l’exposition connexe au risque de l’entreprise.

Principaux aspects

Lors de la planification d’activités continues, la fonction d’audit et d’assurance des SI doit :

- Effectuer et documenter, au moins une fois par an, une Évaluation du risque, afin de faciliter l’élaboration du plan d’audit des SI.
- Inclure dans l’évaluation du risque les plans et objectifs stratégiques de l’organisation et le cadre et les initiatives de gestion du risque de l’entreprise.
- Pour chaque mission d’audit et d’assurance des SI, quantifier et justifier les ressources d’audit des SI nécessaires pour satisfaire aux exigences de la mission.
- Utiliser des évaluations du risque dans la sélection des domaines et éléments présentant un intérêt pour l’audit et les décisions d'audit afin de concevoir et d’exécuter certaines missions d’audit et d’assurance des SI.
- Solliciter l’approbation de l’évaluation du risque auprès des parties prenantes à l’audit et autres parties appropriées.
- Établir des priorités et programmer le travail d’audit et d’assurance des SI sur la base des évaluations du risque.
- À partir de l’évaluation du risque, élaborer un plan qui :
  - Constitue un cadre pour les activités d’audit et d’assurance des SI
  - Prenne en considération les exigences et activités extérieures à l'audit et l'assurance des SI
  - Soit mis à jour au moins une fois par an et approuvé par les personnes en charge de la gouvernance
  - Traite des responsabilités définies par la Charte d’audit

Lors de la planification d’une mission donnée, les professionnels de l’audit et de l’assurance des SI doivent :

- Identifier et évaluer les risques pertinents pour le domaine examiné.
- Pour chaque mission, effectuer une évaluation préliminaire du risque afférent au domaine examiné. Les objectifs de chaque mission doivent refléter les résultats de l’évaluation préliminaire du risque.
- Lors de l’étude des domaines de risque et de la planification d’une mission donnée, étudier les audits, revues et conclusions antérieurs, ainsi que les éventuelles activités correctives. Prendre aussi en considération le processus d’évaluation globale du risque du conseil.
- Tenter de réduire le Risque d'audit à un niveau acceptable et de réaliser les objectifs d’audit par une évaluation appropriée de l’objet SI et des contrôles correspondants, pendant la planification et l'exécution de l'audit des SI.

- Lors de la planification d'une procédure d'audit SI donnée, reconnaître que plus le seuil de Matérialité est bas, les attentes de l'audit sont précises et le risque d'audit est grand.
- Afin de réduire le risque de matérialité accrue, compenser soit en augmentant les tests des contrôles (pour réduire le risque de contrôle), soit ou parallèlement en étendant les procédures de Test de corroboration (pour réduire le risque de non-détection) pour obtenir des assurances supplémentaires.

Terminologie

Terme	Définition
Charte d'audit	Un document approuvé par les personnes chargées de la gouvernance qui définit l'objectif, les pouvoirs et responsabilités de l'activité d'audit interne La charte doit : • Établir la position de la fonction d'audit interne au sein de l'entreprise • Autoriser l'accès aux documents, biens personnels et physiques pertinents pour l'exécution des missions d'audit et d'assurance des SI • Définir la portée des activités de la fonction d'audit
Risque d'audit	Le risque de parvenir à une conclusion inexacte sur la base des résultats de l'audit. Les trois composantes du risque d'audit sont : • risque de contrôle • risque de non-détection • risque inhérent
Risque lié à l'objet de l'audit	Risque lié au domaine examiné : • Risque commercial (capacité des clients à payer, solvabilité, facteurs de marché, etc.) • Risque contractuel (responsabilité, prix, type, pénalités, etc.) • Risque pays (politique, environnemental, de sécurité, etc.) • Risque lié au projet (ressources, ensemble de compétences, méthodologie, stabilité du produit, etc.) • Risque lié à la technologie (solution, architecture, réseau d'infrastructure matérielle et logicielle, circuits de diffusion, etc.) Voir risque inhérent.
Risque de contrôle	Le risque d'existence d'une erreur significative qui ne serait pas empêchée ou détectée en temps opportun par le système de contrôle interne. (Voir risque inhérent.)
Risque de non-détection	Le risque que les procédures de corroboration du professionnel de l'audit ou de l'assurance des SI ne détectent pas une erreur susceptible d'être importante, seule ou combinée à d'autres erreurs. Voir risque d'audit.

Risque inhérent	Le niveau de risque ou l'exposition au risque sans tenir compte des actions entreprises ou susceptibles d'être entreprises par la direction (ex. mise en œuvre de contrôles). Voir risque de non-contrôle.
Matérialité	Un concept d'audit concernant l'importance d'un élément d'information eu égard à son impact ou son effet sur le fonctionnement de l'entité auditée. Une expression de la matérialité d'un élément particulier dans le contexte de l'entreprise dans son ensemble
Évaluation du risque	Un processus utilisé pour identifier et évaluer le risque et ses effets potentiels Des évaluations du risque sont utilisées pour identifier les éléments ou domaines qui présentent les risques les plus importants, la plus grande vulnérabilité ou l'exposition au risque la plus marquée pour l'entreprise, afin de les inclure dans le plan d'audit annuel des SI. Des évaluations du risque sont également utilisées pour gérer la livraison du projet et le risque d'avantages du projet.
Test de corroboration	Obtention d'éléments probants pour l'audit sur l'intégrité, l'exactitude ou l'existence d'activités ou transactions pendant la période d'audit

Lien vers les directives

Type	**Titre**
Directive	2202 Évaluation du risque dans la planification

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.