Norme d'audit et d'assurance des SI 1008 - Critères

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 1008 - Critères

Déclarations

1008.1 **Les professionnels de l'audit et de l'assurance des SI doivent sélectionner des critères d'évaluation de l'objet qui soient objectifs, complets, pertinents, mesurables, compréhensibles, largement reconnus, qui fassent autorité et qui soient compris par, ou à la disposition de, tous les lecteurs et utilisateurs du rapport.**

1008.2 **Les professionnels de l'audit et de l'assurance des SI considéreront la source des critères et se concentreront sur les critères émis par les organismes faisant autorité avant d'accepter des critères moins connus.**

Principaux aspects

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

- Étudier le choix de Critères avec soin et être en mesure de justifier ce choix.
- Faire preuve de jugement professionnel pour s'assurer que, s'ils sont appliqués, les critères permettront d'élaborer une opinion ou une conclusion juste et objective qui ne sera pas trompeuse pour le lecteur ou l'utilisateur. Il est reconnu que la direction peut faire valoir des critères ne remplissant pas toutes les exigences.
- Considérer le caractère adéquat et la disponibilité de critères pour déterminer les exigences de la mission.
- Lorsque les critères ne sont pas facilement disponibles, incomplets ou susceptibles d'interprétation, inclure une description et toute autre information nécessaire pour s'assurer que le rapport est juste, objectif et compréhensible et que le contexte dans lequel les critères sont utilisés est inclus dans le rapport.

Le caractère adéquat et approprié des critères d'évaluation de l'objet doit être évalué par rapport aux cinq critères d'adéquation suivants :

- **Objectivité** – Les critères doivent être exempts de parti pris susceptible d'affecter défavorablement les conclusions du professionnel et, en conséquence, être trompeurs pour l'utilisateur du rapport.
- **Intégrité** – Les critères doivent être suffisamment complets pour que tous les critères susceptibles d'affecter les conclusions du professionnel sur l'objet soient identifiés et utilisés dans la conduite de la mission d'audit ou d'assurance des SI.
- **Pertinence** – Les critères doivent être pertinents eu égard à l'objet et contribuer à l'élaboration de conclusions satisfaisant les objectifs de la mission d'audit ou d'assurance des SI.
- **Mesurabilité** – Les critères doivent permettre une mesure cohérente de l'objet et l'élaboration de conclusions constantes lorsqu'ils sont appliqués par différents professionnels dans des circonstances similaires.
- **Intelligibilité** – Les critères doivent être communiqués clairement et ne pas être susceptibles d'interprétation notablement différente par les utilisateurs pressentis.

L'acceptabilité des critères est affectée par la disponibilité des critères pour les utilisateurs du rapport du professionnel, de sorte que les utilisateurs comprennent la base de l'activité d'assurance et la pertinence des conclusions. Les sources peuvent comprendre celles qui sont :

- **Reconnues** – Les critères doivent être suffisamment reconnus pour que leur utilisation ne soit pas contestée par les utilisateurs pressentis.

Principaux aspects (suite)

- **Faisant autorité** – Il convient de rechercher des critères correspondant à ceux des autorités de référence dans le domaine et qui soient appropriés eu égard à l'objet. Par exemple, les critères énoncés par les autorités de référence peuvent provenir d'organismes professionnels, de groupes sectoriels, de l'État et des autorités de réglementation.
- **À la disposition du public** – Les critères doivent être à la disposition des utilisateurs du rapport du professionnel. Les exemples comprennent les normes élaborées par des organismes professionnels d'expertise comptable et d'audit comme l'ISACA, l'IFAC (International Federation of Accountants) et d'autres organismes publics ou professionnels reconnus.
- **À la disposition de tous les utilisateurs** – Si des critères ne sont pas à la disposition du public, ils doivent être communiqués à tous les utilisateurs par le biais d'affirmations incorporées au rapport du professionnel. Les affirmations sont constituées de déclarations sur l'objet qui répondent aux exigences de critères adéquats pour qu'ils puissent être audités.

Outre l'adéquation et la disponibilité, la sélection de critères d'assurance des SI doit également prendre en considération la source, en termes d'utilisation et de public potentiel. Par exemple, s'agissant de réglementations édictées par l'État, des critères fondés sur des affirmations élaborées à partir de la législation et des réglementations qui s'appliquent à l'objet peuvent s'avérer les plus appropriés. Dans d'autres cas, des critères sectoriels ou d'associations professionnelles peuvent être pertinents. Les sources de critères possibles sont, par ordre dans lequel elles doivent être envisagées :

- **Critères établis par l'ISACA** – Ce sont des critères et normes à la disposition du public, qui ont été exposés à des vérifications professionnelles et à un processus de vérifications préalables exhaustif par des experts internationaux reconnus dans les domaines de la gouvernance informatique, du contrôle, de la sécurité et de l'assurance.
- **Critères établis par d'autres groupes d'experts** – Ces critères, similaires aux normes et critères de l'ISACA, sont pertinents en ce qui concerne l'objet et ont été élaborés et exposés à des vérifications professionnelles et à un processus de vérifications préalables exhaustif par des experts dans divers domaines.
- **Critères établis par les lois et réglementations** – Bien que les lois et réglementations puissent fournir la base de critères, il convient de les utiliser avec le plus grand soin. Il arrive souvent que leur rédaction soit complexe et porteuse d'un sens juridique précis. Dans de nombreux cas, il peut être nécessaire de reformuler les exigences sous forme d'affirmations. En outre, l'expression d'une opinion sur une disposition législative est généralement limitée aux seuls membres de la profession juridique.
- **Critères établis par des entreprises qui ne suivent pas la procédure établie** – Ils comprennent des critères pertinents élaborés par d'autres entreprises qui n'ont pas suivi la procédure établie et n'ont pas été soumis à consultation et débat publics.
- **Critères élaborés expressément pour la mission d'audit ou d'assurance des SI** – Bien que des critères élaborés expressément pour la mission d'audit ou d'assurance des SI puissent être appropriés, il convient de prêter un soin particulier à s'assurer qu'ils remplissent les critères d'adéquation, en particulier d'intégrité, de mesurabilité et d'objectivité. Les critères élaborés expressément pour une mission d'audit ou d'assurance des SI revêtent la forme d'affirmations.

Les critères de sélection doivent être étudiés avec soin. Le respect de la législation et des réglementations locales est important et doit être considéré comme obligatoire. Il est toutefois reconnu que de nombreuses missions d'audit et d'assurance des SI comprennent des domaines, comme la gestion du changement, les contrôles informatiques généraux et les contrôles d'accès, qui ne sont pas couverts par la loi ou les réglementations. En outre, certains secteurs d'activité, comme celui des cartes de paiement, ont établi des exigences obligatoires qui doivent être respectées. Lorsque des exigences législatives reposent sur des principes, le professionnel doit s'assurer que les critères sélectionnés correspondent à l'objectif de la mission.

Au fur et à mesure de la progression de la mission, des informations supplémentaires peuvent rendre certains critères inutiles pour atteindre les objectifs. Dans ce cas, il n'est pas nécessaire d'effectuer de travaux supplémentaires en rapport avec ces critères.

Terminologie

Terme	Définition
Critères	Les normes et points de référence utilisés pour mesurer et présenter l'objet et par rapport auxquels l'auditeur SI évalue l'objet. Les critères doivent être : • Objectifs – exempts de parti pris • Complets – comprendre tous les facteurs pertinents pour parvenir à une conclusion • Pertinents – se rapporter à l'objet • Mesurables – permettre des mesures cohérentes Dans une mission d'attestation, ce sont des points de référence par rapport auxquels l'affirmation écrite de la direction sur l'objet peut être évaluée. Le praticien tire une conclusion sur l'objet en se référant à des critères appropriés.

Lien vers les directives

Type	Titre
Directive	2008 Critères

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.

