

S16 E-COMMERCE

Le caractère spécialisé de l'audit des systèmes d'information (SI) et les compétences requises pour effectuer un tel audit rendent nécessaire la mise en œuvre de normes qui s'appliquent spécifiquement à cette discipline. Un des objectifs d'ISACA[®] consiste à proposer des normes mondialement applicables conformes à son optique. Le développement et la promulgation de Normes d'audit des SI sont des pierres angulaires de la contribution de l'ISACA à la communauté des auditeurs. La structure des Normes d'audit des SI fournit de nombreux niveaux d'assistance :

- Les **Normes** définissent des exigences obligatoires en matière d'audit des SI et de reporting. Elles informent :
 - Les auditeurs 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 concernées 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 **Directives** apportent des instructions sur l'application des Normes d'audit des SI. L'auditeur des SI doit s'y référer au moment de mettre en œuvre les normes, faire appel à son jugement professionnel avant de les appliquer et se préparer à justifier tout écart vis-à-vis d'elles. Les Directives d'audit des SI visent à fournir de plus amples informations sur la manière de se conformer aux normes applicables.
- Les **Procédures** constituent des exemples de méthodes qu'un auditeur des SI peut appliquer lors d'une mission d'audit. La documentation des procédures contient des informations sur la mise en œuvre des normes d'audit des SI, mais ne fixe pas d'obligations. Les Procédures d'audit des SI visent à fournir de plus amples informations sur la manière de se conformer aux normes applicables.

COBIT[®] (Control Objectives for Information and related Technology, Objectifs de contrôle pour l'information et les technologies associées) est un cadre de gouvernance et un ensemble d'outils de support des technologies de l'information (TI) qui permet aux gestionnaires de combler le fossé qui sépare les exigences en matière de contrôle, les problèmes techniques et les risques commerciaux. COBIT permet un développement clair des stratégies et des bonnes pratiques pour le contrôle des TI dans les organisations. Il met l'accent sur la conformité aux règlements, il aide les organisations à augmenter la valeur obtenue grâce à l'IT, permet l'alignement et simplifie la mise en œuvre des concepts du cadre COBIT.

Le modèle COBIT est destiné aux dirigeants et aux responsables des TI, mais aussi aux auditeurs des SI. Par conséquent, son utilisation permet de comprendre les objectifs de l'entreprise, de faire connaître les bonnes pratiques et d'émettre des recommandations autour d'une référence normative comprise et respectée de tous. COBIT peut être téléchargé à partir du site Web ISACA, www.isaca.org/cobit. Comme le précise la structure du COBIT, chacun des produits et/ou éléments associés suivants est organisé par processus de gestion TI :

- **Objectifs de contrôle**—Déclarations génériques de contrôle de qualité minimale liées aux processus TI.
- **Directives de gestion**—Instructions visant à évaluer et à améliorer la performance des processus TI à l'aide de modèles de maturité, de diagrammes RACI (Responsabilité, Autorité, Consulté et/ou Informé) d'objectifs et de métrologie. Elles constituent une structure orientée gestion pour l'auto-évaluation des contrôles continus et proactifs spécifiquement centrée sur :
 - La mesure des performances
 - La définition du profil des contrôles des TI
 - La sensibilisation
 - L'étalement concurrentiel
- **Pratiques de contrôle COBIT**—Déclarations de risque et de valeur et instructions de mise en œuvre pour les objectifs de contrôle
- **IT Assurance Guide**—Instructions relatives à chaque zone de contrôle sur la manière de comprendre les problématiques, d'évaluer chaque contrôle, de mesurer la conformité et de quantifier le risque de contrôles non satisfaisants

Un **glossaire** est à disposition sur le site Internet de l'ISACA à l'adresse www.isaca.org/glossary. Les mots audit et révision sont interchangeables dans les Normes, Directives et Procédures d'audit des SI.

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. Au moment de déterminer la propriété d'une procédure ou d'un test spécifique, le professionnel du contrôle doit faire appel à son propre jugement professionnel en fonction des circonstances, des systèmes impliqués ou de l'environnement technologique.

Le Comité de normalisation de l'ISACA s'engage à réaliser une vaste consultation pour préparer les Normes, Directives et Procédures d'audit des SI. Avant d'éditer ses documents, le Comité de normalisation publie des exposés-sondages à l'échelle internationale pour recueillir les avis du grand public. Si nécessaire, le Comité de normalisation consulte également des personnalités dont l'expertise ou l'intérêt dans le domaine abordé est susceptible d'apporter un éclairage utile. Dans le cadre de son programme de développement continu, le Comité de normalisation encourage les membres de l'ISACA et toutes les parties intéressées à lui signaler les problèmes émergents qui nécessitent l'établissement de nouvelles normes. Envoyer les suggestions par courrier électronique (standards@isaca.org), par télécopie (+1 847 253 1443) ou par courrier postal (adresse à la fin de ce document) au siège international de l'ISACA, à l'attention du directeur de la recherche normative et des relations avec les universités. Date de publication du présent document : 1er décembre 2007.

S16 E-commerce

Introduction

- 01 Les Normes de l'ISACA contiennent des principes de base et des procédures essentielles obligatoires, indiqués en lettres noires en caractères gras, ainsi que les instructions associées.
- 02 L'objet de cette norme ISACA est d'établir des normes et de fournir des instructions concernant l'examen d'environnements de e-commerce.

Norme

- 03 L'auditeur des SI doit évaluer les contrôles applicables et évaluer le risque lors de l'examen d'environnements de e-commerce afin de s'assurer que les transactions d'e-commerce sont contrôlées correctement.**

Commentaire

- 04 Le e-commerce est défini comme les processus au moyen desquels les organisations traitent des affaires par voie électronique avec leurs clients, leurs fournisseurs et autres partenaires commerciaux extérieurs, en utilisant Internet comme outil technologique. Il inclut par conséquent les modèles d'e-commerce B2B (business-to-business) et B2C (business-to-consumer).
- 05 L'auditeur des SI doit utiliser une technique ou une approche d'évaluation des risques appropriée pour développer le plan général d'audit des SI, lequel devrait inclure la couverture des environnements d'e-commerce.
- 06 L'auditeur des SI doit envisager l'utilisation de techniques d'analyse des données y compris l'utilisation d'assurance permanente, qui permet aux auditeurs des SI de surveiller en permanence la fiabilité des systèmes et de réunir des éléments sélectifs probants de l'audit via l'ordinateur lors de l'examen des activités d'e-commerce.
- 07 Le niveau d'aptitudes et de connaissances nécessaire pour comprendre les implications de contrôle et de gestion des risques de l'e-commerce varie avec la complexité des activités d'e-commerce de l'organisation.
- 08 L'auditeur des SI doit comprendre la nature et le caractère critique du processus d'entreprise pris en charge par l'application d'e-commerce avant de démarrer l'audit afin que les résultats puissent être évalués dans un contexte adéquat.
- 09 Se référer aux instructions suivantes pour plus d'informations sur l'e-commerce :
- Directive G21 Examen des systèmes d'ERP (Enterprise Resource Planning)
 - Directive G22 Examen de l'e-commerce B2C (Business-to-consumer)
 - Directive G24 Services bancaires par Internet
 - Directive G25 Examen des VPN (Virtual Private Networks, réseaux privés virtuels)
 - Directive G33 Considérations générales sur l'utilisation de l'Internet
 - Procédure P6 Pare-feu
 - Structure COBIT et objectifs de contrôle

Date de prise d'effet

- 10 La présente Norme ISACA s'appliquera aux audits de SI débutant à compter du 1^{er} février 2008.

Comité 2007-2008 de normalisation de l'ISACA

Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Capco IT Services India Private Limited, India
Brad David Chin, CISA, CPA Google Inc., États-Unis
Sergio Fleginsky, CISA ICI Paints, Uruguay
Maria Gonzalez, CISA HomeLand Office, Espagne
John Ho Chi, CISA, CISM, CBCP, CFE Ernst & Young, Singapour
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australie
John G. Ott, CISA, CPA AmerisourceBergen, États-Unis
Jason Thompson, CISA, CIA KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA Microsoft Corp., États-Unis

© 2007 ISACA. Tous droits réservés.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 États-Unis
Téléphone : +1 847 253 1545
Télécopie : +1 847 253 1443
E-mail : standards@isaca.org
Site Web : www.isaca.org