



Information Systems
Audit and Control
Association

NORME D'AUDIT DES SYSTÈMES D'INFORMATION

CHARTRE D'AUDIT

DOCUMENT N° S1

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 spécifiquement adaptées à cette discipline. L'un des objectifs de l'ISACA® (Information Systems Audit and Control Association® – Association de l'audit et du contrôle des systèmes d'information) est de 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 en matière d'agissements des praticiens
 - Les titulaires de la certification CISA® (Certified Information Systems Auditor® – Auditeur informatique agréé) 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.

Les ressources du COBIT® constituent un modèle de bonnes pratiques. La *structure* du COBIT précise : « Les dirigeants ont pour responsabilité de préserver l'ensemble des actifs de l'entreprise. Pour exercer cette responsabilité et atteindre ses objectifs, les dirigeants doivent établir un système de contrôle interne adapté. » Le référentiel COBIT fournit un ensemble détaillé de contrôles et de techniques de contrôle destiné aux environnements de gestion des systèmes d'information. Dans le COBIT, le choix des éléments les plus pertinents pour un audit particulier est basé sur la sélection de processus TI spécifiques et sur la prise en compte des critères d'information du COBIT.

Comme le précise la *structure* du COBIT, chacun des éléments suivants est organisé par processus de gestion TI. 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 meilleures pratiques et d'émettre des recommandations autour d'une référence normative comprise et respectée de tous. Le COBIT inclut :

- Des objectifs de contrôle — Déclarations génériques détaillées et de haut niveau pour un contrôle de qualité minimale
- Des pratiques de contrôle — Justifications pratiques et instructions de mise en œuvre pour les objectifs de contrôle
- Des directives d'audit — 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
- Des directives de gestion — Instructions sur la manière d'évaluer et d'améliorer les performances des processus TI à l'aide de la métrologie, de modèles de maturité et de facteurs de succès essentiels. Elles constituent une structure orientée gestion pour l'auto-évaluation des contrôles continus et proactifs spécifiquement centrée sur :
 - La mesure des performances — Jusqu'à quel point la fonction TI répond-elle aux besoins de l'entreprise ? Les directives de gestion permettent de mettre en œuvre des ateliers d'auto-évaluation, mais aussi d'assurer l'application par les dirigeants de procédures de vérification et d'amélioration continues dans le cadre d'un plan de gouvernance TI.
 - Définition du profil des contrôles TI — Quels sont les processus TI importants ? Quels sont les facteurs de succès essentiels d'un contrôle ?
 - Sensibilisation — Quels sont les risques que les objectifs ne soient pas atteints ?
 - Étalonnage concurrentiel — Que font les autres ? Comment mesurer et comparer les résultats ? Les directives de gestion proposent des exemples de métrologie au service de l'évaluation des performances TI en entreprise. Les indicateurs d'objectifs essentiels soulignent et mesurent les résultats des processus TI et les indicateurs de performances essentiels évaluent l'efficacité des processus en quantifiant les éléments favorables. Les modèles et attributs de maturité assurent l'évaluation des capacités et l'étalonnage concurrentiel. Ils aident les dirigeants à mesurer les capacités de contrôle, mais aussi à identifier les besoins de vérification et les stratégies d'amélioration.

Un **glossaire** est à disposition sur le site Internet de l'ISACA à l'adresse www.isaca.org/glossary. Dans ce glossaire, les termes « audit » et « review » sont interchangeables.

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 : 15 octobre 2004.

Charte d'audit S1

Introduction

- 01 Les Normes de l'ISACA contiennent des principes de base et des procédures essentielles obligatoires, indiqués en caractères gras, ainsi que les instructions associées.
- 02 La présente Norme d'audit des SI a pour objectif l'établissement et la promulgation d'instructions concernant la Charte d'audit applicable durant le processus d'audit.

Norme

- 03 L'objectif, la responsabilité, l'autorité et l'imputabilité de la fonction et des missions d'audit des systèmes d'information doivent être documentés de manière adéquate dans une charte d'audit ou une lettre de mission.**
- 04 La charte d'audit ou la lettre de mission doit être avalisée au niveau approprié au sein de l'entreprise concernée.**

Commentaire

- 05 S'agissant de la fonction d'audit interne des systèmes d'information, une charte d'audit doit être préparée pour les activités en cours. La charte d'audit doit faire l'objet de révisions annuelles ou plus fréquentes si les responsabilités viennent à être partagées ou modifiées. L'auditeur interne des SI peut utiliser une lettre de mission pour clarifier plus avant ou confirmer les implications dans des missions spécifiques d'audit ou de non-audit. S'agissant d'un audit externe des SI, une lettre de mission doit normalement être préparée pour chaque mission d'audit ou de non-audit.
- 06 La charte d'audit ou la lettre de mission doit être suffisamment détaillée pour communiquer l'objectif, les responsabilités et les limites de la fonction ou de la mission d'audit.
- 07 La charte d'audit ou la lettre de mission doit être révisée régulièrement pour vérifier que l'objectif et les responsabilités ont été correctement documentés.
- 08 Se référer aux instructions suivantes pour plus d'informations sur la préparation d'une charte d'audit ou d'une lettre de mission :
- Directive d'audit des SI G5, Charte d'audit
 - Structure COBIT, objectif de contrôle M4

Date de prise d'effet

- 09 La présente Norme ISACA s'appliquera à tous les audits de systèmes d'information débutant à compter du 1^{er} janvier 2005 inclus.

Association de l'audit et du contrôle des systèmes d'information 2004-2005 Comité de normalisation

Président, Sergio Fleginsky, CISA	PricewaterhouseCoopers, Uruguay
Svein Aldal	Aldal Consulting, Norvège
John Beveridge, CISA, CISM, CFE, CGFM, CQA	Office of the Massachusetts State Auditor, États-Unis
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP	Value Partners, Italie
Christina Ledesma, CISA, CISM	Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP	Brisbane City Council, Australie
V. Meera, CISA, CISM, ACS, CISSP, CWA	Microsoft Corporation, États-Unis
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	NextLinx India Private Ltd., Inde
Peter Niblett, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, Australie
John G. Ott, CISA, CPA	Aetna Inc., États-Unis
Thomas Thompson, CISA	Ernst & Young, Émirats Arabes Unis

© Copyright 2004

Information Systems Audit and Control Association

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