Fraude

Guide de gestion du risque de fraude

SYNTHÈSE

COSO
Committee of Sponsoring Organizations of the Treadway Commission

Principaux auteurs

David L. Cotton, CPA, CFE, CGFM
Président, Cotton & Company LLP

Sandra Johnigan, CPA/CFF, CFE
Fondatrice, Johnigan, P.C.

Leslye Givarz, CPA
Réviseur technique, Public Company Accounting Oversight Board (retraité)

Remerciements

Le COSO et l'ACFE remercient l'ensemble des membres du comité consultatif et du groupe de travail sur la gestion du risque de fraude (voir page iv) d'avoir généreusement accepté de donner de leur temps et de partager leurs ressources et leur savoir.

Le COSO et l'ACFE remercie sincèrement David L. Cotton, président du groupe de travail sur la gestion du risque de fraude, pour son remarquable leadership et ses efforts en vue de l'achèvement de ce guide.

Membres du Conseil du COSO

Robert B. Hirth, Jr.
COSO Chair

Douglas F. Prawitt, Ph.D., CPA
American Accounting Association

Charles Landes, CPA
American Institute of CPAs (AICPA)

Mitchell A. Danaher, CMA
Financial Executives International

Sandra Richtermeyer, Ph.D., CMA, CPA
Institute of Management Accountants

Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
The Institute of Internal Auditors

Préface

Ce projet a été commandité par le COSO (Committee of Sponsoring Organizations of the Treadway Commission) qui, de par son leadership incontestable, a vocation à élaborer des référentiels et des lignes directrices de premier plan concernant la gestion des risques, le contrôle interne et la lutte contre la fraude. Ces référentiels sont destinés à améliorer les performances et la gouvernance de l'organisation et à réduire l'étendue de la fraude dans les organisations. Le COSO est une initiative privée, parrainée et financée conjointement par les organisations suivantes :

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.

COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)
aaahq.org

American Institute of CPAs (AICPA)

Fraude

Guide de gestion du risque de fraude

SYNTHÈSE

Décembre 2016

Étude commanditée par

COSO

Committee of Sponsoring Organizations of the Treadway Commission

Avant-propos

En 1992, le COSO *(Committee of Sponsoring Organizations of the Treadway Commission)* a publié *La pratique du contrôle interne*. Ce premier guide a été très largement accepté et utilisé dans le monde entier. Il est reconnu comme un référentiel faisant autorité pour la conception, la mise en place et le pilotage du contrôle interne, ainsi que pour l'évaluation de son efficacité.

Le COSO a révisé le référentiel initial en 2013[1] (le « *Référentiel* »). Dix-sept principes y sont énoncés[2]. Associés aux cinq composantes du contrôle interne, ils fournissent à l'utilisateur des indications claires sur la conception et la mise en place des systèmes de contrôle interne. Ils facilitent en outre la compréhension des conditions nécessaires à l'efficacité du contrôle interne. Le COSO précise qu'un système de contrôle interne efficace suppose que chacun des dix-sept principes soit mis en place et fonctionne conjointement.

Le principe n° 8, l'un des principes de la composante « Évaluation des risques », énonce que :
L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles d'affecter la réalisation des objectifs.

Le présent *Guide de gestion du risque de fraude,* cohérent avec le *Référentiel* qu'il complète, propose des bonnes pratiques pour l'application de ce nouveau principe d'évaluation du risque de fraude.

Pour les organisations qui souhaitent adopter une approche plus globale de la gestion du risque de fraude, ce guide contient davantage de recommandations que les seules informations nécessaires pour réaliser une évaluation du risque de fraude. Il propose également des lignes directrices pour la mise en place d'un programme global de gestion du risque de fraude, notamment :

- l'élaboration d'une politique de gouvernance en matière de risque de fraude ;
- la réalisation d'une évaluation du risque de fraude ;
- la conception et la mise en œuvre d'activités de contrôle préventif et détectif de la fraude ;
- la conduite d'investigations ;
- le pilotage et l'évaluation du programme de gestion du risque de fraude dans son ensemble.

Ce guide est conçu pour parler aux utilisateurs du *Référentiel* du COSO. Il contient des principes et des points d'attention[3]. Ses cinq principes sont cohérents avec les cinq composantes du contrôle interne[4] et les dix-sept principes du COSO.

Ce guide reprend et met à jour un document de 2008 publié et commandité par l'*American Institute of CPAs* (AICPA), l'*Institute of Internal Auditors* (IIA), et l'*Association of Certified Fraud Examiners* (ACFE). Cette précédente version, intitulée *Managing the Business Risk of Fraud: A Practical Guide*, contenait des recommandations similaires pour la mise en œuvre d'un programme global de gestion du risque de fraude et a été utilisée par de nombreuses organisations pour gérer le risque de fraude. Le COSO salue le travail réalisé par le comité de rédaction à l'origine de cette publication. Ce nouveau guide reprend la trame de la précédente version et se propose de la mettre à jour tenant compte des évolutions récentes, de la réviser à des fins de cohérence avec les nouveaux termes utilisés par le COSO, et d'y ajouter des informations importantes liées aux évolutions technologiques – notamment à l'analyse des données.

[1] NdT : Ce *Référentiel* a été publié en français sous l'intitulé « Référentiel intégré de contrôle interne. Principes de mise en œuvre et de pilotage » chez Eyrolles en 2014

[2] Selon le Référentiel du COSO, les principes « correspondent aux concepts fondamentaux associés à chaque composante du contrôle interne ».

[3] Selon le Référentiel du COSO, les points d'attention correspondent à « des caractéristiques importantes des principes ».

[4] Selon le Référentiel du COSO, une composante est « l'un des cinq éléments du contrôle interne. Les cinq composantes sont les suivantes : environnement de contrôle, évaluation des risques, activités de contrôle, information et communication, pilotage ».

La synthèse de ce guide offre une vue d'ensemble destinée au Conseil et à la direction générale. Elle présente les avantages de la mise en œuvre de dispositifs de contrôle et de politiques robustes en matière de lutte contre la fraude. Les annexes contiennent un grand nombre de modèles, d'exemples et d'outils utiles pour aider les utilisateurs à mettre en œuvre les bonnes pratiques exposées dans ce guide.

En outre, ce guide contient des liens hypertextes vers un certain nombre de modèles et d'outils automatisés précieux pour la mise en œuvre et la documentation d'un programme global et efficace de gestion du risque de fraude.

Le COSO a également publié *Le management des risques de l'entreprise* (référentiel ERM). Le présent guide, le *Référentiel intégré de contrôle interne* du COSO et le référentiel ERM sont complémentaires. Selon la manière dont les organisations mettent en œuvre ces trois publications, certains aspects pourront se recouper ou s'imbriquer. Le risque de fraude peut toucher des domaines en dehors de la comptabilité et de la gestion financière. En fait, une organisation qui souhaite minimiser les conséquences négatives de la fraude, devra examiner le risque de fraude à tous les niveaux et dans toutes ses activités.

Le Conseil du COSO adresse ses remerciements aux membres du groupe de travail qui ont contribué à l'élaboration de ce guide, au comité consultatif qui a revu l'ébauche et formulé de précieux commentaires, ainsi qu'au Comité consultatif du COSO qui a contribué à la révision du guide.

Enfin, le Conseil du COSO souhaite vivement remercier David L. Cotton, président du groupe de travail, pour son remarquable leadership et ses efforts en vue de l'achèvement de ce guide.

Robert B. Hirth, Jr.
COSO Chair

James D. Ratley
ACFE President et CEO

Groupe de travail sur la gestion du risque de fraude

Barbara Andrews
AICPA

Michael Birdsall
Comcast Corporation

Toby Bishop
Précédemment ACFE,
Deloitte

Margot Cella
Center for Audit Quality

David Coderre
CAATS

David L. Cotton,
Président
Cotton & Company LLP

James Dalkin
GAO

Ron Durkin
Durkin Forensic, Inc.

Bert Edwards
Formerly State
Department

Frank Faist
Charter Communications

Eric Feldman
Affiliated Monitors, Inc.

Dan George
USAC

John D. Gill
ACFE

Leslye Givarz
Précédemment AICPA,
PCAOB

Cindi Hook
Comcast Corporation

Sandra K. Johnigan
Johnigan, PC

Bill Leone
Norton Rose Fulbright

Andi McNeal
ACFE

Linda Miller
GAO

Kemi Olateju
General Electric

Chris Pembroke
Crawford & Associates, PC

J. Michael Peppers
University of Texas

Kelly Richmond Pope
DePaul University

Carolyn Devine Saint
University of Virginia

Jeffrey Steinhoff
KPMG

William Titera
Précédemment EY

Michael Ueltzen
Ueltzen & Company

Pamela Verick
Protiviti

Vincent Walden
EY

Bill Warren
PwC

Richard Woodford
U.S. Coast Guard
Investigative Service

Panel consultatif sur la gestion du risque de fraude

Dan Amiram
Columbia University Business School

Zahn Bozanic
The Ohio State University

Greg Brush
Tennessee Comptroller of Treasury

Tamia Buckingham
Massachusetts School Building Authority

Ashley L. Comer
James Madison University

Molly Dawson
Cotton & Company LLP

Eric Eisenstein
Cotton & Company LLP

Michael Justus
University of Nebraska

Theresa Nellis-Matson
New York Office of the State Comptroller

Jennifer Paperman
New York Office of the State Comptroller

Daniel Rossi
New York Office of the State Comptroller

Lynda Harbold Schwartz
Upland Advisory LLC

Rosie Tomforde
Regional Government

Le Conseil du COSO souhaite vivement remercier David L. Cotton, président du groupe de travail sur la gestion du risque de fraude, pour son remarquable leadership et ses efforts en vue de l'achèvement de ce guide.

Synthèse | Gestion du risque de fraude

Une fraude est tout acte intentionnel ou toute omission intentionnelle ayant pour but de tromper autrui, et qui entraîne une perte pour la victime et/ou un avantage pour le fraudeur[5].

Chaque organisation est confrontée au risque de fraude. Il est impossible d'éliminer toutes les fraudes dans toutes les organisations. Cependant, la mise en œuvre des principes de ce guide maximisera la probabilité qu'une fraude soit prévenue et détectée en temps voulu et suscitera un fort effet dissuasif.

Le Conseil[6], la direction générale et l'ensemble des collaborateurs à tous les échelons de l'organisation – les managers et leurs collaborateurs à tous niveaux hiérarchiques ainsi que les auditeurs internes – ont la responsabilité de gérer le risque de fraude. Ils doivent notamment : comprendre la position adoptée par l'organisation pour faire face à l'accroissement des risques, au durcissement des réglementations, ainsi qu'à l'attention de l'opinion publique et de leurs parties prenantes ; savoir quel programme de gestion du risque de fraude elle a mis en place ; savoir comment elle identifie les risques de fraude ; connaître les mesures qu'elle applique pour mieux prévenir la fraude, ou du moins pour la détecter au plus tôt ; et connaître les processus existants pour enquêter sur la fraude et mettre en œuvre des mesures correctives. Le présent guide de gestion du risque de fraude est conçu pour aider les organisations à appréhender ces problématiques complexes.

Ce guide fournit au Conseil, à la direction générale, à l'ensemble des collaborateurs et aux auditeurs internes des recommandations pour lutter contre la fraude dans leur organisation. La lutte contre la fraude est un processus visant à éliminer les facteurs qui peuvent favoriser la fraude. Elle est effective lorsqu'une organisation met en œuvre un dispositif de gestion du risque de fraude qui comprend :

- l'élaboration d'un processus de gouvernance rigoureux et visible en matière de lutte contre la fraude ;
- l'instauration d'une culture de la transparence et d'intransigeance contre la fraude ;
- la mise en place d'une évaluation périodique approfondie du risque de fraude ;
- la conception, l'application et l'actualisation de processus et procédures de contrôle préventif et détectif de la fraude ;
- la mise en œuvre rapide d'actions en réponse à des allégations de fraude, y compris, le cas échéant, envers les personnes impliquées dans des malversations.

Le présent guide fournit des lignes directrices de mise en œuvre déterminant des principes et des points d'attention[7] en matière de gestion du risque de fraude et explique comment des organisations de tailles et de catégories différentes peuvent élaborer leur propre programme de gestion du risque de fraude. Il inclut des exemples de ressources et de composantes clés que les organisations peuvent utiliser comme point de départ pour élaborer un tel programme avec efficience et efficacité. En outre, le guide renvoie à d'autres références permettant d'adapter le programme de gestion du risque de fraude selon le type d'organisation (secteur d'activité, public ou à but non lucratif). Chaque organisation doit évaluer l'importance à accorder à la gestion du risque de fraude en fonction de sa taille et de son contexte.

Ce guide contient également de précieuses informations pour les utilisateurs qui mettent en œuvre un processus de gestion du risque de fraude. Il décrit par exemple les rôles et les responsabilités dans ce domaine, détaille les éléments à prendre en compte pour les petites organisations, étudie le recours à l'analyse de données, et analyse la gestion du risque de fraude dans le secteur public.

[5] Les auteurs ont conçu cette définition pratique pour les besoins du présent guide tout en reconnaissant l'existence de nombreuses autres définitions de la fraude, notamment de l'*Auditing Standards Board de l'American Institute of Certified Public Accountants*, du *Public Company Accounting Oversight Board,* ou du *Government Accountability Office*.

[6] Tout au long de ce guide, le terme « Conseil » désigne l'organe de gouvernance ou de surveillance de l'organisation.

[7] Selon le *Référentiel intégré de contrôle interne* du COSO (Eyrolles, 2014), les principes « correspondent aux concepts fondamentaux associés à chaque composante » du contrôle interne. Les points d'attention correspondent quant à eux à des « caractéristiques importantes des principes ».

Lien entre les cinq composantes et les dix-sept principes du contrôle interne du Référentiel du COSO et les cinq principes de gestion du risque de fraude du présent guide

En 2013, le COSO a révisé son référentiel intégré de contrôle interne publié en 1992 pour y faire figurer dix-sept principes. Ces principes sont associés aux cinq composantes du contrôle interne établies par le COSO. Les cinq principes de gestion du risque de fraude du présent guide concordent parfaitement avec les dix-sept principes du contrôle interne énoncés dans le *Référentiel* du COSO[8]. La corrélation entre les principes de gestion du risque de fraude et les composantes et principes du contrôle interne du *Référentiel* du COSO se présente comme suit :

Composantes et principes du *Référentiel* du COSO		Principes de gestion du risque de fraude
Environnement de contrôle	1. L'organisation démontre son engagement en faveur de l'intégrité et des valeurs éthiques. 2. Le Conseil fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne. 3. Le management, agissant sous la surveillance du Conseil, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour atteindre les objectifs. 4. L'organisation démontre son engagement à attirer, former et fidéliser des personnes compétentes conformément aux objectifs. 5. L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne afin d'atteindre les objectifs.	1. L'organisation définit et diffuse un programme de gestion du risque de fraude qui traduit les attentes du Conseil et de la direction générale et démontre leur engagement en faveur d'un niveau élevé d'intégrité et de valeurs éthiques en matière de gestion du risque de fraude.
Évaluation des risques	6. L'organisation définit des objectifs de façon suffisamment claire pour permettre l'identification et l'évaluation des risques susceptibles d'affecter leur réalisation. 7. L'organisation identifie les risques susceptibles d'affecter la réalisation de ses objectifs dans l'ensemble de son périmètre et procède à leur analyse de façon à déterminer comment ils doivent être gérés. 8. L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles d'affecter la réalisation des objectifs. 9. L'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle interne.	2. L'organisation réalise des évaluations globales du risque de fraude pour identifier les risques de fraude qui lui sont propres, estimer leur probabilité et leur importance, évaluer les activités de contrôle existantes, et mettre en œuvre des dispositifs de maîtrise des risques résiduels de fraude.
Activités de contrôle	10. L'organisation sélectionne et développe des activités de contrôle qui visent à maîtriser et à ramener à un niveau acceptable les risques susceptibles d'affecter la réalisation des objectifs. 11. L'organisation sélectionne et développe des contrôles généraux informatiques pour faciliter la réalisation des objectifs. 12. L'organisation déploie des activités de contrôle par le biais de règles qui précisent les objectifs poursuivis, et de procédures qui permettent de mettre en œuvre ces règles.	3. L'organisation sélectionne, développe et déploie des activités de contrôle préventif et détectif de la fraude pour maîtriser le risque de survenance ou de non-détection en temps voulu.
Information et communication	13. L'organisation obtient, produit et utilise des informations pertinentes et de qualité pour faciliter le fonctionnement du contrôle interne. 14. L'organisation communique en interne l'information nécessaire au bon fonctionnement du contrôle interne, notamment les informations relatives aux objectifs et aux responsabilités du contrôle interne. 15. L'organisation communique aux tiers les éléments qui peuvent affecter le fonctionnement du contrôle interne.	4. L'organisation met en place un processus de communication pour obtenir des informations sur les fraudes potentielles et déploie une approche coordonnée en matière d'investigations et de mesures correctives pour traiter la fraude de manière appropriée et en temps voulu.
Pilotage	16. L'organisation sélectionne, développe et réalise des évaluations continues et/ou ponctuelles pour s'assurer que les composantes du contrôle interne sont mises en place et fonctionnent.	5. L'organisation sélectionne, développe et réalise des évaluations pour s'assurer que les cinq principes de gestion du risque de fraude sont mis en place et fonctionnent, et communique les déficiences du programme de gestion du risque de fraude en temps voulu aux responsables des mesures correctives, y compris, le cas échéant, à la direction générale et au Conseil.

[8] Les dix-sept principes du contrôle interne du Référentiel du COSO ont été adoptés par l'État fédéral américain dans son livre vert *Standards for Internal Controls in the Federal Government*, publié par le Contrôleur général des États-Unis. La loi sur l'intégrité des gestionnaires financiers d'organismes fédéraux de 1982 *(Federal Managers' Financial Integrity Act)* impose aux agences fédérales de se conformer aux normes édictées par le Contrôleur général. En outre, le GAO *(Government Accountability Office)* a publié un référentiel de gestion des risques de fraude dans les programmes fédéraux, élaboré à partir de pratiques reconnues sous la forme d'un outil permettant aux agences fédérales de concevoir leur propre programme de gestion du risque de fraude. [Cf. gao.gov/assets/680/671664.pdf.]

Le lien le plus évident entre les deux séries de principes se situe au niveau du principe n° 8 du *Référentiel* du COSO (L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles d'affecter la réalisation des objectifs) et du principe n° 2 de ce guide (L'organisation réalise des évaluations globales du risque de fraude pour identifier les risques de fraude qui lui sont propres, estimer leur probabilité et leur importance, évaluer les activités de contrôle existantes, et mettre en œuvre des dispositifs de maîtrise des risques résiduels de fraude). En outre, comme le montre le tableau précédent, tous les principes du *Référentiel* du COSO sont liés aux principes de gestion du risque de fraude et ils se corroborent mutuellement.

Synthèse des composantes et des principes de gestion du risque de fraude

Gouvernance relative au risque de fraude

La gouvernance relative au risque de fraude fait partie intégrante de la **gouvernance** de l'organisation et de **l'environnement de contrôle**. La gouvernance correspond à la manière dont le Conseil et la direction générale remplissent leurs obligations respectives pour que l'organisation réalise ses objectifs notamment ses responsabilités envers les parties prenantes en matière fiduciaire, de reporting et juridique.

L'environnement de contrôle établit un cadre propice à l'évaluation des risques susceptibles d'affecter la réalisation des objectifs.

Environement de contrôle

Principe n° 1

L'organisation élabore et diffuse un programme de gestion du risque de fraude qui traduit les attentes du Conseil et de la direction générale et démontre leur engagement en faveur d'un niveau élevé d'intégrité et de valeurs éthiques en matière de gestion du risque de fraude.

Évaluation du risque de fraude

Une évaluation du risque de fraude est un processus dynamique et itératif permettant d'identifier et d'évaluer les risques de fraude spécifiques à l'organisation. L'évaluation du risque de fraude porte sur le risque de reporting financier frauduleux, de reporting extra-financier frauduleux, de **détournement d'actifs** et d'actes illégaux (y compris la corruption). Les organisations peuvent adapter cette approche pour qu'elle réponde à leurs propres besoins tout en tenant compte de leur complexité et de leurs objectifs. L'évaluation du risque de fraude ne fait pas seulement partie intégrante de l'évaluation des risques et du contrôle interne, elle est précisément liée au principe n° 8 du *Référentiel* du COSO.

Évaluation des risques

Principe n° 2

L'organisation réalise des évaluations globales du risque de fraude pour identifier les risques de fraude qui lui sont propres, estimer leur probabilité et leur importance, évaluer les activités de contrôle existantes, et mettre en œuvre des dispositifs de maîtrise des risques résiduels de fraude.

Activité de contrôle de la fraude

Une **activité de contrôle** de la fraude est une action définie par des règles et des procédures qui permet de veiller à ce que les directives du management visant à maîtriser les risques de fraude soient appliquées. Une activité de contrôle de la fraude est une procédure ou un processus spécifique conçu pour empêcher la survenance d'une fraude ou pour la détecter rapidement si elle survient.

Les activités de contrôle de la fraude sont généralement soit préventif (conçu pour empêcher la fraude d'être commise) soit détectif (conçu pour révéler une fraude existante). La sélection, le développement, la mise en œuvre et le pilotage des activités de contrôle préventif et détectif sont essentiels à la gestion du risque de fraude. Les activités de contrôle de la fraude sont documentées et s'accompagnent d'une description du risque de fraude identifié, de l'activité de contrôle de la fraude conçue pour maîtriser ce risque, et de l'identification des responsables de cette activité de contrôle. Les activités de contrôle de la fraude contribuent à l'évaluation continue du risque de fraude dans le cadre du dispositif de contrôle interne.

Activités de contrôle

Principe n° 3

L'organisation sélectionne, développe et déploie des activités de contrôle préventif et détectif de la fraude pour maîtriser le risque de survenance ou de non-détection en temps voulu.

Investigations et mesures correctives

Les activités de contrôle ne peuvent pas fournir une assurance absolue contre la fraude. Par conséquent, l'organe de gouvernance veille à ce que l'organisation développe et mette en place un système rapide, confidentiel et performant de revue, d'investigation et de résolution des cas de non-conformité et des allégations de fraude et de manquement.

Une organisation peut améliorer ses opportunités de recouvrement de pertes et limiter son exposition aux litiges et aux atteintes à sa réputation en établissant et en planifiant soigneusement son dispositif d'investigation et de mesures correctives.

Information et communication

Principe n° 4

L'organisation met en place un processus de communication pour obtenir des informations sur les fraudes potentielles et déploie une approche coordonnée en matière d'investigation et de mesures correctives pour traiter la fraude de manière appropriée et en temps voulu.

Pilotage de la gestion du risque de fraude

Le cinquième principe de gestion du risque de fraude porte sur le pilotage du processus global de gestion du risque de fraude. C'est ainsi que les organisations peuvent s'assurer que les cinq principes de gestion du risque de fraude sont mis en place et fonctionnent tel que prévu, et que l'organisation identifie les changements nécessaires en temps voulu.

Les organisations ont recours à des évaluations continues et/ou ponctuelles (périodiques) pour piloter la gestion du risque de fraude. Comme dans le *Référentiel* du COSO, l'intégration des évaluations continues d'un programme de gestion du risque de fraude au cœur des **processus métier** à tous les niveaux de l'organisation, permet de disposer d'informations en temps voulu. En outre, certaines organisations mènent périodiquement des évaluations ponctuelles dont le périmètre et la durée varient en fonction de nombreux facteurs, notamment le résultat des évaluations continues.

Pilotage

Principe n° 5

L'organisation sélectionne, développe et réalise des évaluations pour s'assurer que les cinq principes de gestion du risque de fraude sont mis en place et fonctionnent, et communique les déficiences du programme de gestion du risque de fraude en temps voulu aux responsables des mesures correctives, y compris, le cas échéant, à la direction générale et au Conseil.

Gestion efficace du risque de fraude

Le *Référentiel* du COSO précise qu'un système de contrôle interne efficace suppose que chacun des dix-sept principes soit mis en place et fonctionne conjointement.

Le principe n° 8, l'un des principes de la composante « Évaluation des risques », énonce que :
L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles d'affecter la réalisation des objectifs.

Ce guide, cohérent avec le *Référentiel* du COSO qu'il complète, propose des bonnes pratiques pour réaliser une évaluation du risque de fraude.

Recommandations pour l'utilisation du guide de gestion du risque de fraude

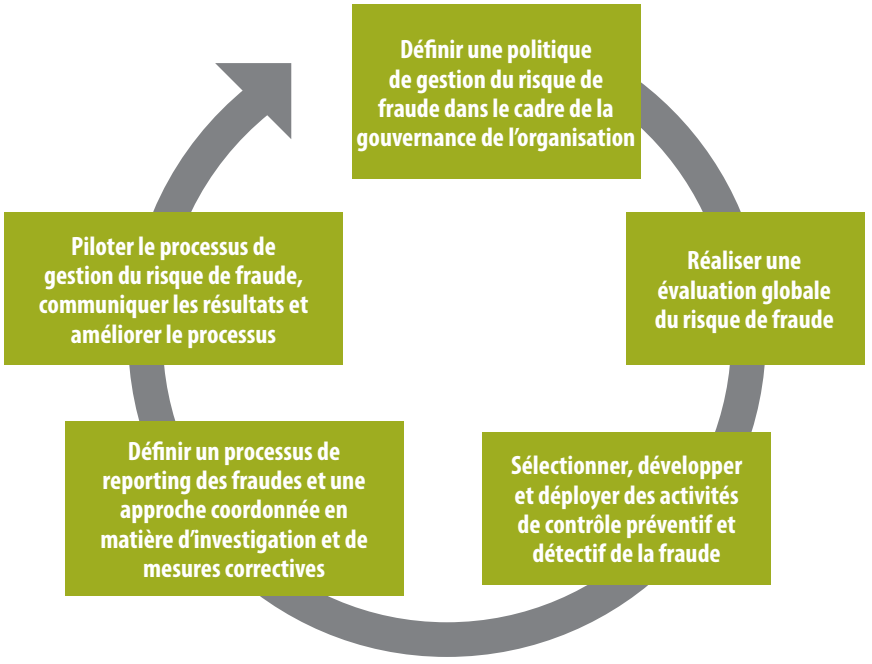
Ce guide est conçu pour être utilisé par tous types d'organisations, quels que soient leur statut (public, privé, gouvernemental, universitaire, à but non lucratif), leur taille ou leur secteur d'activité. Bien entendu, chaque organisation adaptera les principes qu'il contient. Les petites organisations et les organisations gérées par leur propriétaire sans organe de gouvernance peuvent adapter ce guide à leur propre situation. Les pouvoirs publics ont des structures de gouvernance très différentes, avec des responsables élus, des représentants de l'État, et des nominations politiques au plus haut niveau.

Les termes utilisés sont génériques et peuvent être adaptés à l'organisation qui souhaite mettre en œuvre ces principes. Par exemple, et comme indiqué précédemment, le guide utilise les termes « Conseil » ou « organe de gouvernance » pour désigner l'organe chargé de la surveillance de la direction générale et de la gouvernance, indépendamment de son appellation dans une organisation donnée.

Les auteurs de ce guide recommandent aux organisations appliquant le *Référentiel* du COSO d'appréhender les lignes directrices de ce guide comme un dispositif distinct, compatible et plus exhaustif pour l'évaluation spécifique du risque de fraude dans l'organisation, dans le cadre d'un programme ou d'un processus global de gestion du risque de fraude. Outre l'évaluation du risque de fraude, cette approche englobe la gouvernance du risque de fraude, la conception et la mise en œuvre d'activités de contrôle de la fraude, la conduite d'investigations et de mesures correctives, ainsi que l'évaluation et le pilotage de la gestion du risque de fraude. Les résultats de la mise en œuvre des recommandations de ce guide étayeront et seront cohérents avec ceux du *Référentiel* du COSO.

Cette approche rigoureuse se traduit par la mise en œuvre d'un dispositif global et continu de gestion du risque de fraude comme suit :

Figure 1. Dispositif global et continu de gestion du risque de fraude



Cette approche globale reconnaît et met l'accent sur la différence fondamentale entre une déficience du contrôle interne entraînant une **erreur** et une déficience entraînant une **fraude**, à savoir son **caractère intentionnel**. Une organisation qui ne fait qu'ajouter l'évaluation du risque de fraude à son évaluation du contrôle interne risque de ne pas mener un examen exhaustif et de ne pas identifier les possibilités d'actes intentionnels visant à :

- falsifier la présentation des informations financières
- falsifier la présentation des informations extra-financières
- détourner des actifs
- perpétrer des actes illégaux ou de corruption

La mise en œuvre d'une évaluation spécifique et davantage axée sur le risque de fraude dans le cadre d'un processus de gestion du risque de fraude distinct permet un meilleur ciblage des actes intentionnels.

Cette approche globale est également susceptible de déboucher sur une évaluation plus exhaustive et plus fiable du risque de fraude. Elle fournit des éléments supplémentaires pour une gestion globale du risque de fraude. Si les organisations utilisent l'approche simplifiée (et se limitent à réaliser l'évaluation du risque de fraude), elles peuvent combiner ces résultats avec ceux du *Référentiel* du COSO pour renforcer leurs dispositifs de détection et de prévention.

Utilisation par les parties prenantes concernées

Conseil et comité d'audit

Un Conseil engagé et performant discute avec la direction générale du programme de gestion du risque de fraude de l'entité et fournit une surveillance, si nécessaire. La responsabilité globale de la conception et de la mise en œuvre du programme de gestion du risque de fraude incombe à la direction générale, qui doit notamment faire preuve d'exemplarité pour faire émerger une culture commune au sein de l'organisation. Le Conseil établit des politiques et des procédures pour expliquer comment s'exerce sa surveillance, et il fixe notamment ses attentes en termes d'intégrité et de valeurs éthiques, de transparence, et de devoir de rendre compte concernant la mise en œuvre et le fonctionnement du programme de gestion du risque de fraude. À l'issue de ses évaluations du risque de fraude, la direction générale informe le Conseil des risques résiduels de fraude, et de toute fraude avérée ou suspectée. Le Conseil procède à une critique constructive de la direction générale et n'hésite pas, le cas échéant, à poser les questions qui dérangent. Il recueille des informations auprès des auditeurs internes, des auditeurs externes, évaluateurs externes et des experts juridiques, et exploite si besoin ces ressources pour investiguer tout soupçon.

Direction générale

La direction générale évalue le programme de gestion du risque de fraude de son entité au regard du présent guide, en se concentrant sur la manière dont l'organisation applique les cinq principes associés à ce programme. Elle évalue en outre le risque de fraude de l'entité en lien avec le principe n° 8 du *Référentiel* du COSO.

Managers et collaborateurs

Les managers et les collaborateurs s'interrogent sur la manière dont ils exercent leurs responsabilités à la lumière de ce guide et partagent avec leurs supérieurs hiérarchiques des pistes pour renforcer les contrôles relatifs au risque de fraude. Plus précisément, ils examinent la manière dont les contrôles existants affectent les principes associés aux cinq composantes de la gestion du risque de fraude, ainsi que le principe n° 8 du *Référentiel* du COSO.

Audit interne

Les auditeurs internes revoient leur plan d'audit interne et la manière dont celui-ci prend en compte le programme de gestion du risque de fraude de l'entité en lien avec la mise en œuvre des présentes recommandations. Ils passent ce guide en revue et envisagent les conséquences des modifications apportées au programme de gestion de risque de fraude de l'entité sur le plan d'audit, les évaluations d'audit, et le reporting relatif à la gestion du risque de fraude de l'entité et à son système de contrôle interne.

Auditeurs externes

Il n'est pas rare qu'un auditeur externe soit tout à la fois chargé par un client d'auditer ou d'examiner l'efficacité du contrôle interne relatif au reporting financier et d'auditer les états financiers de l'entité. Le principe n° 8 du *Référentiel* du COSO précise que l'organisation intègre le risque de fraude dans son évaluation des risques susceptibles d'affecter la réalisation des objectifs. Avec ce guide, les auditeurs externes peuvent évaluer la mise en œuvre de ce principe par l'entité.

Autres organisations professionnelles

Les autres organisations professionnelles qui élaborent des lignes directrices sur le risque de fraude lié aux opérations, au reporting et à la conformité peuvent comparer leurs normes et leurs lignes directrices au présent guide. Il est dans l'intérêt de toutes les parties de limiter les divergences de concepts et de terminologie.

Formateurs

En admettant qu'ils soient largement acceptés, les concepts et les dispositions du présent guide devraient trouver leur place dans des programmes de formation initiale ou continue.

Fraude

Guide de gestion du risque de fraude

SYNTHÈSE

COSO
Committee of Sponsoring Organizations of the Treadway Commission

Fraude

Guide de gestion du risque de fraude

SYNTHÈSE

COSO
Committee of Sponsoring Organizations of the Treadway Commission