10 Gestion des risques

Ce chapitre commente le principe de la gestion des risques figurant dans la recommandation du Conseil de l'OCDE sur l'intégrité publique. Dans une perspective tant gouvernementale qu'institutionnelle, il explore la manière dont les organes du secteur public peuvent adapter leurs politiques et leurs pratiques pour gérer efficacement les risques liés à l'intégrité, mener des évaluations de risques et maintenir un environnement de contrôle qui préserve l'intégrité publique. Il souligne également la nécessité de procédures cohérentes pour lutter contre les menaces de fraude ou de corruption, notamment de protocoles pour le signalement, le suivi et les enquêtes. Ce chapitre examine également le rôle essentiel des fonctions d'audit interne dans leurs relations aux administrateurs du gouvernement, en se concentrant sur leur valeur ajoutée qui consiste à fournir une assurance indépendante et objective pour un contrôle interne et une gestion efficaces des risques liés à l'intégrité. Le chapitre met en évidence les principaux défis et les pratiques exemplaires, comme l'élaboration de politiques de contrôle interne fondées sur les valeurs, la mise en place d'évaluations périodiques des risques liées aux objectifs et la création de boucles de rétroaction pour suivre et évaluer les activités.

10.1. Pourquoi une gestion des risques ?

Pour les organismes du secteur public, disposer d'un système de contrôle interne et d'un cadre de gestion des risques est essentiel au succès de toute stratégie d'intégrité publique. Des politiques et des processus efficaces de contrôle interne et de gestion des risques renforcent les défenses des organismes du secteur public contre la fraude et la corruption, et garantissent un fonctionnement optimal des gouvernements dans la mise en œuvre des programmes d'intérêt public. En outre, ces politiques et processus contribuent à garantir l'optimisation des ressources et à faciliter la prise de décision. Solidement établis, ils aident les gouvernements à trouver un équilibre entre un modèle axé sur l'application de la loi et des approches plus préventives, fondées sur les risques.

Le contrôle interne et la gestion des risques couvrent une série de mesures visant à prévenir et détecter la fraude et la corruption et à y répondre. Ces mesures comprennent des politiques, des pratiques et des procédures qui permettent à l'administration et au personnel d'assurer leur rôle de protection de l'intégrité en évaluant correctement les risques et en élaborant des mesures de contrôle basées sur le risque. Des mécanismes de réaction aux cas de corruption et de violation des normes d'intégrité sont également essentiels pour un système de contrôle interne intégré.

Dans cette perspective, la Recommandation de l'OCDE sur l'intégrité publique appelle les adhérents à « appliquer un cadre interne de contrôle et de gestion des risques pour protéger l'intégrité au sein des entités du secteur public, notamment :

a. en garantissant un environnement de contrôle assorti d'objectifs clairs qui démontrent l'attachement des responsables à l'intégrité publique et aux valeurs du service public, cet environnement offrant un niveau d'assurance raisonnable quant à l'efficience et aux résultats de l'entité et à sa conformité avec les lois et les usages ;
b. en garantissant une approche stratégique de la gestion des risques qui consiste notamment à évaluer les risques pour l'intégrité publique, à combler les lacunes en matière de contrôle (en particulier en intégrant des dispositifs d'avertissement dans les processus d'importance critique) et à mettre en place un mécanisme efficient de suivi et d'assurance-qualité du système de gestion des risques ;
c. en veillant à ce que les mécanismes de contrôle soient cohérents et intègrent des procédures clairement définies qui permettent de donner suite aux soupçons fondés de violation de la législation et de la réglementation, et en facilitant le signalement des abus aux autorités compétentes sans crainte de représailles » (OCDE, 2017[1]).

10.2. Qu'est-ce que la gestion des risques ?

Le contrôle interne et la gestion des risques permettent aux organes du secteur public d'atteindre un large éventail de buts et d'objectifs politiques. Le principe relatif à la gestion des risques se concentre sur les aspects du contrôle interne et de la gestion des risques dans le contexte de la préservation de l'intégrité et de la lutte contre la corruption dans le secteur public. Les gouvernements doivent en dernier lieu adapter leur approche à leurs contextes juridiques, réglementaires et culturels respectifs. Cela implique l'intégration des objectifs d'intégrité dans les politiques et pratiques existantes en matière de contrôle interne et de gestion des risques. Il s'agit également d'adapter les normes et concepts internationaux de contrôle interne et de gestion des risques aux réalités locales et au secteur public, dont les normes et orientations produites par le Committee of Sponsoring Organizations de la Commission Treadway (COSO), l'Organisation internationale de normalisation, l'Institut des auditeurs internes (par exemple le modèle des « trois lignes de défense ») et l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI).

Un système de contrôle interne est une composante intégrée aux opérations d'un organe du secteur public. Du point de vue de l'intégrité publique, le contrôle interne et la gestion des risques consistent en des politiques, des processus et des mesures de gestion des risques de fraude, de corruption et d'abus (ci-après dénommés collectivement les « risques liés à l'intégrité »). Les éléments suivants sont des composantes essentielles d'un système de contrôle interne conçu pour préserver l'intégrité :

- un environnement de contrôle efficace[1] et une gestion des risques liés à l'intégrité.
- une approche adaptée de la gestion et de l'évaluation des risques liés à l'intégrité.
- un suivi et une évaluation de la gestion des risques liés à l'intégrité.
- des procédures cohérentes et réactives dans le cadre du contrôle interne et de la gestion des risques.
- une fonction d'audit interne qui fournit une garantie et des conseils indépendants et objectifs pour renforcer le contrôle interne et la gestion des risques liés à l'intégrité.

Pour être mis en œuvre efficacement, ces composantes reposent sur de nombreux acteurs aux niveaux gouvernemental, institutionnel et individuel. Par exemple, les organes de normalisation du secteur public peuvent veiller à ce que les politiques de contrôle interne et de gestion des risques à l'échelle du gouvernement soient cohérentes et harmonisées, comme évoqué plus loin. Au niveau institutionnel, les politiques et processus de contrôle interne et de gestion des risques fournissent à l'administration une assurance raisonnable que l'organisation atteint ses objectifs d'intégrité et gère ses risques efficacement. Les composantes du contrôle interne et de la gestion des risques sont également présentes au niveau individuel : de nombreuses normes appellent à l'engagement personnel des agents publics en faveur de l'intégrité et du respect des codes de conduite.

10.2.1. Un environnement de contrôle efficace et une gestion des risques liés à l'intégrité

Au sein des organes du secteur public, l'environnement de contrôle sert un large éventail d'objectifs financiers, budgétaires et de performances. Il est constitué d'un ensemble de normes, de processus et de structures de contrôle interne à l'échelle d'une entité (Committee of Sponsoring Organizations of the Treadway Commission, 2013[2]). Au-delà du respect de la législation, des normes et autres exigences, l'environnement de contrôle et les processus qui le constituent contribuent à la bonne gouvernance et aident les organes du secteur public à fournir des résultats aux citoyens d'une manière efficace et efficiente. Dans le contexte du principe de gestion des risques, l'environnement de contrôle reflète les objectifs, les politiques et les personnes qui contribuent à institutionnaliser un système d'intégrité, de prise de décisions éthiques et de gestion des risques.

Considérations à l'échelle du gouvernement pour un environnement de contrôle fondé sur l'intégrité

À l'échelle du gouvernement, la responsabilité de la mise en œuvre du contrôle interne et de la gestion des risques est partagée par différents organes du secteur public. Ces organes comprennent le centre du gouvernement (CdG), les institutions d'audit, les unités centrales d'harmonisation et les organes de lutte contre la corruption. En particulier, ils : 1) définissent et harmonisent les normes et les politiques de contrôle interne, 2) fournissent des orientations et des outils, 3) évaluent les efforts déployés à l'échelle du gouvernement pour préserver l'intégrité, et 4) coordonnent et normalisent les pratiques de signalement et de réaction aux violations présumées de l'intégrité pour l'ensemble du secteur public. Par exemple, aux États-Unis, l'institution supérieure de contrôle des finances publiques, le Bureau gouvernemental des comptes (Government Accountability Office - GAO), dirige le processus de normalisation du contrôle interne et de gestion des risques en collaboration avec un conseil d'experts, et publie les Normes de contrôle interne du gouvernement fédéral (Bureau gouvernemental des comptes, 2014[3]) ainsi qu'un cadre de pratiques de pointe pour la gestion des risques de fraude au sein du gouvernement (Bureau

gouvernemental des comptes, 2015[4]). Le Bureau de la gestion et du budget fédéraux (Office of Management and Budget - OMB) complète le travail du GAO par des politiques et des orientations de mise en œuvre. Ces dernières comprennent notamment un document (la circulaire OMB n° A-123) qui décrit la responsabilité de l'administration et les exigences liées au contrôle interne et à la gestion des risques au sein du gouvernement fédéral, avec une référence explicite à l'évaluation des risques de fraude (Bureau de la gestion et du budget fédéraux, 2016[5]). En France, toutes les entités publiques (administrations de l'État, collectivités locales, établissements publics et sociétés d'économie mixte) sont légalement tenues de procéder à des évaluations des risques, quelle que soit leur taille. À ce titre, les entités publiques doivent dresser la liste de tous les processus liés à leurs activités, comme le recrutement et les marchés publics, et évaluer les risques liés à l'intégrité associés (encadré 10.1).

Encadré 10.1. Le contrôle interne dans les États membres de l'Union européenne

Les deux principes fondamentaux des normes de contrôle interne public dans les États membres européens sont : 1) le contrôle interne public repose sur le Committee of Sponsoring Organizations de la Commission Treadway (COSO) et l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI), et 2) chaque pays membre devrait avoir une fonction au sein du gouvernement de coordination et d'harmonisation du contrôle et de l'audit internes pour toutes les entités publiques. Par conséquent, même s'il existe divers systèmes de contrôle interne dans les États membres, ils disposent tous d'un organe gouvernemental qui joue le rôle d'harmonisation centrale du contrôle interne.

En outre, les États membres et leurs institutions publiques partagent des normes cohérentes issues des mêmes pratiques internationales de contrôle interne et de gestion des risques. Les normes comportent des dispositions explicites concernant le contrôle interne et la gestion des risques de fraude dans la gestion des fonds de l'UE.

Source : (Commission européenne, 2015[6]).

Un manque de clarté de la part du niveau central sur la méthodologie d'institutionnalisation du contrôle interne et la gestion des risques peut donner l'impression que les objectifs d'intégrité, ainsi que les activités de contrôle interne et de gestion des risques qui les soutiennent, sont distincts des autres objectifs stratégiques et opérationnels. Le CdG, ainsi que d'autres organes ayant des responsabilités à l'échelle du gouvernement, peuvent jouer un rôle essentiel pour aider les organes du secteur public à surmonter ce défi en fournissant des normes, des politiques et des orientations unifiées. Ils peuvent également contribuer à sensibiliser à la valeur du contrôle interne et de la gestion des risques pour la prise de décision et la réalisation des objectifs de l'organe.

Considérations institutionnelles et individuelles pour un environnement de contrôle fondé sur l'intégrité

Les employés, quel que soit le niveau de l'organisation où ils se trouvent, ont des rôles et des responsabilités dans la gestion des risques de fraude et de corruption (Committee of Sponsoring Organizations of the Treadway Commission, 2016[7]). Ce principe peut être spécifié dans les politiques, les procédures et les orientations de l'organisation en matière de contrôle interne et de gestion des risques, ou peut s'articuler comme une politique d'intégrité autonome. Ces politiques, qu'elles s'articulent entre différentes politiques ou s'insèrent dans le cadre d'une politique d'intégrité autonome, ne devraient pas être utilisées comme des listes de contrôle pour se conformer aux normes minimales. Elles doivent être complètes et adaptées à chaque organisation, en tenant compte des risques actuels et émergents liés à

l'intégrité. Les éléments essentiels des politiques visant à promouvoir un environnement de contrôle efficace au sein des organes du secteur public peuvent inclure :

- une référence aux valeurs et principes d'intégrité ainsi qu'aux normes de conduite personnelle qui sous-tendent l'organisation, et à leur signification dans la pratique
- une déclaration des objectifs de l'organisation en matière de lutte contre la fraude et la corruption, en établissant un lien explicite avec la manière dont les activités de contrôle interne et de gestion des risques servent ces objectifs
- une description de l'alignement entre les objectifs d'intégrité et les autres politiques et outils de l'organisation (c'est-à-dire le code de conduite, le code d'éthique)
- une définition de la fraude et de la corruption, avec des exemples d'actions considérées comme constituant un délit de corruption ou de fraude
- l'identification du personnel auquel s'applique la politique, en tenant compte du personnel temporaire et des bénévoles
- des rôles et responsabilités clairement définis en matière de contrôle interne et de gestion des risques liés à la fraude, à la corruption, au gaspillage et aux abus
- la diffusion auprès des employés des méthodes de signalement des actes présumés répréhensibles, des canaux internes de signalement accessibles, et des procédures à suivre
- l'identification des mesures d'exécution et la description de la façon dont les différents types d'actes répréhensibles présumés seront examinés.

L'encadrement a la responsabilité première de créer et de maintenir un environnement de contrôle qui met en avant l'intégrité et instaure un climat positif. En outre, l'engagement des hauts échelons permet de sensibiliser aux risques liés à l'intégrité et contribue à améliorer la mise en œuvre des activités de contrôle. L'encadrement peut inclure les responsables ou des groupes de personnes (par exemple, les conseils ou les comités) responsables de la conception, de la mise en œuvre et du suivi des politiques et des pratiques de contrôle interne et de gestion des risques. En outre, l'encadrement doit faire la preuve de son engagement individuel en faveur de l'intégrité (pour en savoir plus, voir les chapitres 1 et 6). Grâce aux codes de conduite et aux codes d'éthique, l'encadrement peut communiquer ses attentes en matière de comportement intègre, ainsi que les valeurs organisationnelles qui permettent aux individus de démontrer personnellement leur comportement éthique. Ces codes définissent les normes de comportement de base des agents publics et peuvent également servir de base à l'encadrement pour évaluer le respect des codes d'éthique et les faire appliquer, si nécessaire par des mesures disciplinaires (pour en savoir plus, voir le chapitre 4).

Certains organes du secteur public désignent une entité chargée de gérer les risques liés à l'intégrité. Cette entité dédiée peut être un comité, une équipe ou une personne, selon les besoins. Par exemple, dans certains organes, l'entité est un comité qui aide à superviser, coordonner, contrôler et évaluer les activités de gestion des risques dans toute l'organisation. Dans d'autres cas, les organes désignent des gestionnaires des risques liés à l'intégrité ou créent des groupes de travail chargés d'atteindre les objectifs d'intégrité dans l'environnement de contrôle. Le mandat et la taille de l'organe (dont le nombre de programmes et d'employés et les ressources) et la complexité des risques permettent de déterminer si une entité dédiée serait bénéfique. Quelle que soit l'approche adoptée, il est essentiel que l'entité ou la fonction relève directement de l'encadrement supérieur, étant donné la responsabilité globale de cette dernière dans la gestion des risques liés à l'intégrité.

10.2.2. Une approche adaptée de la gestion et de l'évaluation des risques liés à l'intégrité

L'adaptation consiste à façonner les activités de gestion des risques aux conditions particulières d'un organe du secteur public, et à mettre en œuvre des évaluations des risques et des mesures de contrôle adaptées. Les risques liés à l'intégrité varient selon les secteurs et les organisations, et il est donc essentiel

que les organes du secteur public calibrent leurs orientations, leurs outils et leurs approches en fonction de leurs objectifs, de leur environnement et de leurs contextes spécifiques. Cette adaptation est cruciale, étant donné qu'un grand nombre des normes de contrôle interne et de gestion des risques adoptées par les gouvernements ont été initialement élaborées pour le secteur privé. Le CdG, les ministères de tutelle et les personnes responsables de la gestion des risques jouent tous un rôle dans ce processus d'adaptation, ce qui fait l'objet des discussions qui suivent, tant du point de vue du gouvernement que des institutions.

Un soutien ciblé à l'échelle du gouvernement en faveur de la gestion et de l'évaluation des risques liés à l'intégrité

Des orientations et des outils ciblés peuvent aider les gouvernements à orienter leurs activités de contrôle interne et de gestion des risques vers les risques liés à l'intégrité, en reliant ces activités à des objectifs programmatiques plus larges. Ils peuvent également soutenir des stratégies de communication afin que les mesures de contrôle de gestion des risques internes aillent au-delà des simples mesures de contrôle financières et de conformité. Par exemple, en 2010, le Secrétariat du Conseil du Trésor au Canada a élaboré un Cadre de gestion des risques pour guider les directeurs adjoints des ministères dans la mise en œuvre de pratiques de gestion des risques à tous les niveaux de leur organisation. L'Agence française anticorruption (AFA) a publié des directives pour aider les personnes morales publiques et privées à répondre à certaines exigences en matière de lutte contre la corruption et d'intégrité, notamment en procédant à des évaluations des risques. L'AFA a également élaboré des guides techniques spécialisés, par exemple pour les responsables de l'administration des marchés publics. Outre ces directives générales, l'AFA apporte un soutien adéquat aux acteurs publics ou privés qui souhaitent rationaliser leurs procédures de gestion des risques liés à l'intégrité. Des orientations sectorielles, axées sur les domaines à haut risque comme les marchés publics ou la santé, ainsi que des mécanismes de coordination et des outils de compte-rendu pertinents, peuvent aider à combler les lacunes en matière de capacités (encadré 10.2).

Encadré 10.2. Une approche holistique de l'intégrité et un ciblage des domaines à haut risque : le cas de l'Estonie

En Estonie, la stratégie gouvernementale de lutte contre la corruption pour la période 2013-2020 reconnaît les lacunes en matière de prévention de la corruption et d'atténuation des risques dans certains domaines et prévoit des mesures pour y remédier. Elle stipule que le ministère responsable du domaine spécifique en question (par exemple, la santé ou l'environnement) doit également être responsable de la mise en œuvre des mesures de prévention de la corruption spécifiques à son domaine. Pour cibler les domaines à haut risque, le gouvernement estonien a mis en place des réseaux anticorruptions spécifiques à chaque domaine. Chaque ministère dispose d'un coordinateur de prévention de la corruption censé gérer la mise en œuvre de la politique de lutte contre la corruption dans le ministère concerné et dans son domaine de compétence. Les coordinateurs forment le réseau anticorruption – le réseau se réunit environ quatre à cinq fois par an. Le réseau comprend également des représentants de la police, de la société civile, du parlement, de la Cour des comptes et d'autres parties prenantes qui sont invités en fonction du thème choisi. Il existe également un réseau d'autorités sanitaires qui discutent des développements dans leurs domaines respectifs, ainsi que des problèmes à résoudre.

Source : (Ministère de la Justice estonien, 2013[8]).

Les politiques, les processus et les outils permettant de réaliser des évaluations des risques liés à l'intégrité varient d'une organisation à l'autre et dépendent de la taille, du volume d'investissement reçu et du risque auquel est confronté le secteur dans lequel elle opère (par exemple, santé, infrastructure). Par exemple, un organe du secteur public peut procéder à une évaluation indépendante des risques liés à l'intégrité ou intégrer des objectifs d'intégrité dans ses évaluations des risques à l'échelle de l'organe afin de promouvoir l'efficacité. Néanmoins, les politiques de gestion des risques et les processus d'évaluation partagent des caractéristiques similaires dans toutes les organisations. Les politiques de gestion des risques devraient être liées aux objectifs et inclure, entre autres, une description des propositions de gestion des risques, des ressources nécessaires, des responsabilités, des mesures de performances et des exigences en matière de signalement et de suivi (Crime and Corruption Commission, 2018[9]). En outre, comme décrit ci-dessous, la gestion et l'évaluation des risques impliquent généralement un processus itératif en plusieurs étapes consistant à établir le contexte, évaluer et traiter les risques, et assurer un suivi, une communication et une consultation continus (Organisation internationale de la normalisation, 2018[10]).

Établir le contexte de la gestion des risques liés à l'intégrité

La compréhension du contexte interne et externe est une étape essentielle pour les agents publics lorsqu'ils évaluent pour la première fois les facteurs déterminants et les obstacles potentiels à la réalisation des objectifs d'intégrité. Le contexte interne comprend – sans s'y limiter – les objectifs stratégiques, la structure de gouvernance, les rôles, les compétences des employés, les outils opérationnels (par exemple, les données et les systèmes d'information), la culture et les directives internes. Le contexte externe peut comprendre des cadres juridiques et politiques, des parties prenantes externes et des réalités politiques, sociales et économiques qui mettent en exergue des types spécifiques de risques liés à l'intégrité ou de mécanismes de réponse. Ce contexte constitue la base de la conception et de l'amélioration des politiques, des stratégies et des objectifs de gestion et d'évaluation des risques liés à l'intégrité, puisque ni le contexte interne ni le contexte externe ne sont statiques.

Différents outils de planification stratégique peuvent constituer des points de départ utiles pour évaluer le contexte et définir la portée du processus d'évaluation des risques. Par exemple, des outils comme le schéma décisionnel et le diagramme des causes et effets, les cartes de processus et d'influence, et la méthode « PESTLE » (facteurs politiques, économiques, sociologiques, technologiques, juridiques et environnementaux) peuvent faciliter l'analyse tout en favorisant l'engagement des parties prenantes. Des registres des risques à l'échelle du gouvernement ou des ministères peuvent être une contribution utile pour établir le contexte, comme illustré dans l'encadré 10.3.

Encadré 10.3. Développement et gestion de registres des risques – exemple de la Direction des services de santé (HSE - Health Service Executive) en Irlande

La Direction des services de santé élabore des registres des risques afin de gérer ses risques et d'obtenir une vue d'ensemble détaillée du statut des services en matière de risque, à un moment donné. Le registre des risques, qui est un outil très efficace de suivi des risques, décrit le système global des risques et l'état d'avancement des mesures d'atténuation des risques.

Chaque responsable hiérarchique est chargé d'élaborer un registre des risques dans son domaine de responsabilité. Une fois complété, le registre est partagé avec tous les employés de l'entité, de manière explicite et compréhensible, tout en tenant compte de leur niveau de formation, de connaissances et d'expérience. Le plan d'action constitue la partie essentielle d'un registre des risques. Il détaille les mesures supplémentaires nécessaires pour réduire le risque à un niveau satisfaisant. Les mesures supplémentaires qui ne peuvent être gérées au niveau du service doivent être transférées au niveau hiérarchique supérieur.

Le HSE reconnaît que, pour diverses raisons, il est impossible d'éliminer tous les risques. Par conséquent, à n'importe quel stade du processus, on peut décider de « tolérer » ou d'accepter un certain niveau de risque. Lorsqu'un risque ne peut être entièrement éliminé, il doit être consigné dans le registre des risques, accompagné d'une liste de mesures visant à le ramener à un niveau acceptable. Ces risques feront ensuite l'objet d'un suivi régulier. Quatre éléments ont été identifiés en tant que conditions préalables à l'élaboration d'un registre des risques solide :

1. *Disponibilité d'une expertise en matière de risques* – Le personnel qui soutient le processus a besoin d'une formation et d'un enseignement appropriés.
2. *Utilisation de documents et d'outils de soutien approuvés* – Pour garantir la cohérence tout au long du processus, un certain nombre de documents et d'outils approuvés doivent être utilisés lors de l'élaboration d'un registre.
3. *Engagement et appropriation* – L'engagement visible de la part de l'encadrement supérieur, qui peut favoriser l'adhésion des parties prenantes pour garantir la qualité et la durabilité.
4. *Disponibilité d'un soutien sur site* – Un soutien administratif est nécessaire pour l'organisation des ateliers et la coordination générale.

Étant donné que l'évaluation des risques implique un processus dynamique, les risques et leurs mesures de contrôle doivent être examinés, contrôlés et révisés en permanence, le cas échéant.

Source : (Irish Health Service Executive, 2018[11]).

Pour établir le contexte, il faut également identifier les rôles et les responsabilités et mettre en place une équipe chargée d'évaluer les risques liés à l'intégrité dans l'ensemble de l'organisation. Bien qu'il existe des rôles et des fonctions spécifiques au sein des organes du secteur public pour traiter les risques liés à l'intégrité, la gestion des risques nécessite la participation d'un certain nombre d'acteurs. Par exemple, les responsables hiérarchiques, les gestionnaires de risques et les auditeurs internes (c'est-à-dire les première, deuxième et troisième lignes de défense[2], respectivement) jouent tous un rôle essentiel pour garantir que la gestion des risques et le contrôle interne fassent progresser les buts et objectifs de l'organisation.

Tout au long du processus, des mécanismes doivent être mis en place pour assurer la collecte de toutes les données pertinentes et la diffusion des conclusions et des résultats. Grâce à ces données, les organisations peuvent plus facilement intégrer la gestion des risques dans leurs opérations et promouvoir l'appropriation du processus d'évaluation des risques. En Lituanie, par exemple, la loi sur la prévention de la corruption comprend une méthodologie d'analyse des risques de corruption. La méthodologie précise que de nombreuses sources doivent être consultées lors de la réalisation de l'analyse, notamment les résultats des audits et des enquêtes sociales et auprès du personnel (OCDE, 2015[12]).

Le degré d'intégration de la gestion des risques au sein de l'organisation est une autre caractéristique essentielle du contexte interne. Les politiques et pratiques de contrôle interne et de gestion des risques sont plus efficaces lorsqu'elles s'inscrivent dans le cadre de la stratégie et des opérations globales de l'organisation et soutiennent des buts et objectifs concrets. Les modalités précises de cette intégration dépendent de l'organisation. Toutefois, le processus peut inclure la création de liens entre la gestion des risques et les politiques et processus de planification stratégique, de suivi des activités et d'évaluation. Par exemple, au Royaume-Uni, l'administration fiscale et douanière (HM Revenue and Customs) utilise son rapport mensuel sur les performances pour mesurer les progrès réalisés par rapport aux objectifs et pour identifier les domaines de performance qui nécessitent des actions supplémentaires. Un comité de performance, en collaboration avec des « centres de performance », examine les données pertinentes et les principaux risques pour la réalisation des objectifs. Ils examinent en particulier les registres des risques de divers ministères et intègrent les informations et les points de vue sur les risques dans leur évaluation des performances actuelles et existantes (National Audit Office, 2011[13]).

Identifier et analyser les risques liés à l'intégrité

Les évaluations des risques sont des processus itératifs qui permettent à une organisation d'identifier les facteurs qui facilitent ou entravent la réalisation de ses objectifs, en se fondant sur une analyse des risques inhérents[3] et résiduels[4]. Il est essentiel d'établir un lien explicite avec les objectifs afin de guider les personnes qui participent à l'évaluation des risques et de veiller à ce qu'elles ne surchargent pas d'informations le processus et les registres des risques qui en résultent. En fin de compte, les résultats de l'évaluation des risques devraient être utiles à la prise de décision, et le fait de lier des objectifs spécifiques aux risques (par opposition à l'inverse) peut aider les organisations à rester concentrées sur les risques qui comptent. Les évaluations des risques de corruption et de fraude peuvent être des exercices autonomes ou être intégrées aux activités d'évaluation des risques d'une organisation, en reconnaissant les liens entre les différentes catégories de risques, comme les risques stratégiques, opérationnels, financiers, de conformité et de réputation.[5]

Il n'existe aucune approche universelle permettant de mener des évaluations des risques liés à l'intégrité, et il est en fait essentiel de les adapter aux besoins d'une organisation. En général, les organisations peuvent évaluer des risques spécifiques, des facteurs de risque[6], ou une combinaison des deux. Les risques spécifiques sont des systèmes de corruption ou de fraude pertinents qui peuvent avoir un impact sur les objectifs de l'organisation. L'évaluation de ces risques est abordée plus en détail ci-dessous. Les facteurs de risque sont également liés aux objectifs, mais ils renvoient aux caractéristiques des politiques, procédures ou activités de l'organisation qui, une fois évaluées et notées, peuvent mettre en évidence les domaines d'opération à haut risque et, par la suite, définir les priorités. Par exemple, la complexité des procédures peut être un facteur de risque qui peut rendre plus difficile pour une organisation de mener une surveillance efficace et de prévenir la fraude ou la corruption.

Le degré de dépendance d'un contracteur vis-à-vis de ses sous-traitants ou de tiers constitue un autre exemple de facteur de risque, car de nombreux gouvernements engagent régulièrement des contracteurs pour se procurer des biens et des services. Chaque facteur de risque peut être pondéré en fonction des priorités de l'organisation, et noté selon des critères prédéterminés. Par exemple, une organisation peut noter son facteur de risque de dépendance à l'égard de tiers selon les critères du tableau 10.1 suivant. Il est également possible de définir des critères pour d'autres facteurs de risque, comme le budget, la portée de l'impact du programme sur les parties prenantes, la vulnérabilité à la fraude ou le volume et le type de recommandations d'audit reçues.

Tableau 10.1. Exemple de critères des facteurs de risque liés aux tiers

Note	Critères
5	Les processus critiques objectifs sont totalement externalisés
4	Les processus importants dépendent fortement de tiers
3	Les processus sont modérément dépendants de tiers
2	Les tiers exercent certaines activités qui ont un impact sur les objectifs
1	Aucun tiers n'est utilisé, ou n'exerce d'activité essentielle pour atteindre les objectifs

Remarque : 5 = risque élevé ; 1 = risque faible.
Source : Adapté de (Wright Jr., 2013[14]).

Lors de l'évaluation de risques spécifiques, par opposition aux facteurs de risque, les évaluations distinguent généralement les risques inhérents des risques résiduels. Pour mener ces évaluations, une organisation analyserait d'abord les risques inhérents, c'est-à-dire les risques évalués sans mesure de contrôle. Par exemple, dans un premier temps, une organisation évaluerait la probabilité et l'impact de tous les systèmes de fraude potentiels liés à l'utilisation par les employés de cartes de voyage ou de crédit émises par le gouvernement. L'organisation peut utiliser des notes numériques (par exemple, de 1 à 5) pour évaluer la probabilité et l'impact, ou utiliser une classification (par exemple, faible, moyen et élevé). Les scores de probabilité et d'impact peuvent être liés à des critères spécifiques pour faciliter l'évaluation. Par exemple, une organisation évaluant les risques liés à la passation des marchés publics pourrait utiliser les valeurs ou la fréquence des contrats pour mesurer l'impact et classer les risques très élevés (note de 5) par rapport aux risques très faibles (note de 1). Lors du processus d'évaluation des risques, les organisations répéteraient ce processus de notation pour évaluer les risques résiduels.

Le risque résiduel désigne l'exposition au risque après application de mesures d'atténuation. Dans l'exemple précédent, cela inclurait une deuxième phase d'analyse des risques inhérents identifiés, notamment une détermination révisée de la probabilité et de l'impact des risques de fraude compte tenu des mesures de contrôle, comme les procédures relatives aux limites imposées aux cartes de crédit. Comme indiqué dans la section suivante, l'organisation prendrait alors en compte son risque résiduel par rapport aux critères de risque (par exemple, les tolérances[7]), avant de déterminer s'il convient d'apporter des modifications aux activités de contrôle. Lors de l'analyse des risques tant inhérents que résiduels, les organisations doivent éviter l'écueil commun consistant à identifier et à analyser les mesures de contrôle ou les conséquences au lieu des risques qui pourraient saper la réalisation des objectifs.

Pour soutenir les formes qualitatives d'analyse des risques, les organisations disposent de différentes sources. L'analyse des résultats d'audits, les entretiens avec les employés, la réalisation d'évaluations des risques de contrôle et d'analyses d'écart de forces, faiblesses, opportunités, menaces (FFOM) sont des méthodes courantes pour identifier les risques potentiels. D'autres techniques consistent à consulter le registre des risques du pays ou de l'organisation, s'il existe, afin d'identifier les tendances ou les mécanismes en cours qui indiquent une activité frauduleuse ou de corruption. Par ailleurs, les évaluations des risques sont un travail d'équipe. Il peut être utile de faire participer les employés de l'ensemble de l'organisation pour bénéficier de perspectives différentes et pour valider les résultats. Les cadres et les

employés de première ligne – directement responsables des opérations ou de la prestation de services, comme un gestionnaire de contrat en contact direct avec les fournisseurs ou un agent de santé qui interagit avec des bénéficiaires – peuvent avoir des perceptions différentes de la probabilité et de l'impact des risques. Les employés de première ligne peuvent être mieux placés que les cadres pour identifier les risques émergents.

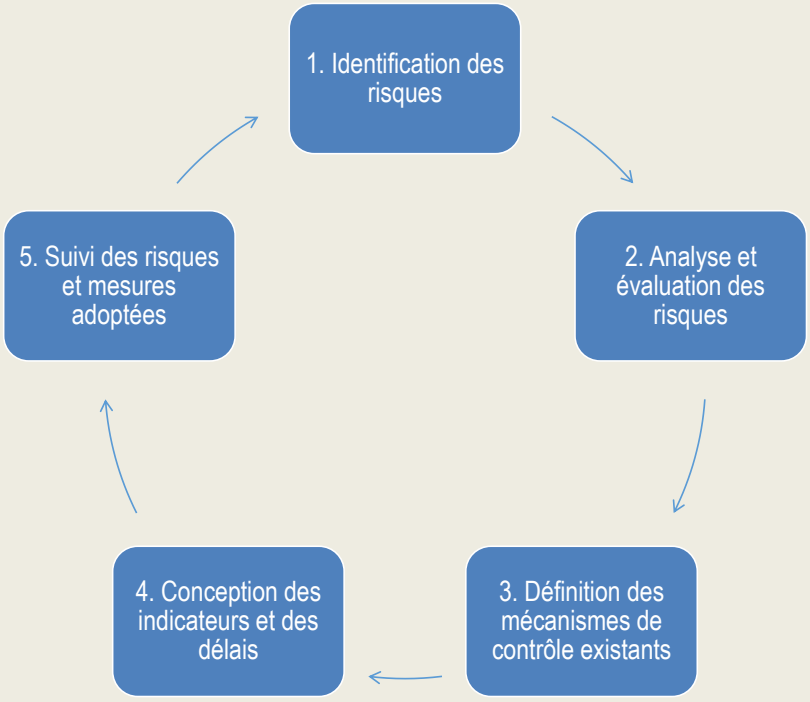
L'utilisation de techniques quantitatives et d'analyses de données permet également d'identifier les fraudes et la corruption potentielles dans une série de domaines où les gouvernements collectent généralement des données fiables et valables. Cela comprend les projets de travaux publics, les marchés publics, les salaires, les services sociaux, les prestations de santé et les services d'emploi. Toutefois, les approches quantitatives peuvent utiliser des ressources considérables et nécessitent souvent des compétences spécialisées et des investissements dans les infrastructures informatiques, les logiciels et la formation. Avant d'investir massivement dans des approches quantitatives ou fondées sur des données pour évaluer les risques, les institutions peuvent envisager des analyses de rentabilité et des possibilités de piloter de nouvelles approches.

Les organisations qui évaluent efficacement les risques adaptent le processus à leur propre environnement et procèdent régulièrement à des évaluations, bien que la fréquence de ces évaluations varie entre les différentes entités. L'encadré 10.4 illustre la manière dont les autorités de la République slovaque procèdent à l'analyse des risques de fraude et de corruption.

Encadré 10.4. Le processus d'évaluation des risques adopté par les autorités de la République slovaque qui mettent en œuvre les Fonds structurels et d'investissement européens (FSIE)

En République slovaque, les autorités responsables de la mise en œuvre des programmes opérationnels (PO) dans le cadre des Fonds structurels et d'investissement européens (FSIE) ont mis en place des procédures de gestion des risques spécifiques qui servent de base à l'évaluation des risques. Conformément aux procédures, la gestion des risques comprend cinq phases interconnectées, parmi lesquelles figure l'évaluation des risques (voir le graphique 10.1). Un élément important de ce processus est la boucle de retour d'information qui illustre la nature itérative des évaluations des risques et l'apprentissage continu des activités de suivi.

Graphique 10.1. Le processus d'évaluation des risques en République slovaque



La première phase consiste à identifier les risques potentiels susceptibles d'affecter négativement la réalisation des objectifs des programmes opérationnels ; ils sont classés dans un catalogue des risques, exhaustifs ou sélectionnés. Les risques de fraude et de corruption sont inclus. Les risques sont ensuite analysés et évalués en fonction de leur importance et de la probabilité de leur occurrence à l'aide de matrices de risques qui permettent de déterminer le niveau de risque global. Les risques de fraude et de corruption possédant un niveau de risque global supérieur à 4 sont désignés par l'équipe d'évaluation des risques comme importants et critiques. Ensuite, les risques sont classés dans leurs catalogues de risques respectifs, et une liste restreinte est établie pour les risques critiques. Les procédures de gestion des risques pour chaque programme opérationnel définissent le traitement approprié des risques après identification et évaluation.

Source : Présenté par des représentants du ministère de l'Environnement de la République slovaque à Bratislava, en février 2019.

Évaluation des risques et stratégie d'atténuation

Après avoir identifié et évalué les risques liés à l'intégrité, y compris les risques inhérents et résiduels, l'étape suivante consiste à déterminer s'il faut y répondre et comment. Cette phase consiste à évaluer les résultats de l'analyse des risques par rapport à des critères de risque spécifiques (c'est-à-dire les tolérances), puis à affiner la stratégie d'atténuation des risques de l'organisation. Les « critères de risque » font référence au niveau de risque qu'une organisation est prête à accepter. En effet, les tolérances sont des critères qui font office de seuils pour faciliter la prise de décision et garantir des mesures de contrôle efficaces et proportionnées.

Les gestionnaires doivent déterminer ces critères avant de procéder à l'évaluation des risques. Les conseils d'administration, les comités d'audit et les responsables peuvent tous être impliqués dans la définition des critères de risque afin de veiller à ce qu'ils soient définis aussi objectivement que possible et en accord avec les politiques, les réglementations et les objectifs de l'organisation. La « tolérance zéro » en matière de corruption et de fraude n'est pas un critère de risque utile. Il est vrai que ce message peut servir de principe directeur et contribuer à promouvoir une culture de la prise de risque. Toutefois, entre autres conséquences imprévues, elle peut également avoir un effet paralysant sur le processus d'évaluation des risques si elle génère une réticence chez les gestionnaires à fournir des informations exactes sur les risques perçus dans leur secteur d'activité. Contrairement aux déclarations de tolérance zéro, les critères de risque spécifiques au contexte ont des implications plus concrètes pour l'évaluation et l'adaptation des activités de contrôle.

Il est irréaliste d'espérer identifier et traiter tous les risques de fraude et de corruption. Les critères de risque doivent être définis de manière à permettre à une organisation de comprendre pleinement un problème et de mettre en place des mesures d'atténuation (Fountain, 2015[15]). Les critères de risque permettent aux cadres de décider s'ils doivent accepter, éviter, réduire ou partager le risque. Si les mesures de contrôle sont efficaces pour maintenir le risque au niveau ou en dessous du seuil fixé par les critères de risque (par exemple, les processus où les risques de fraude interne sont inférieurs à une valeur financière donnée), alors l'acceptation du risque résiduel pourrait être la ligne de conduite la plus efficace en termes de ressources. S'il est établi que les activités de contrôle ne parviennent pas à réduire les risques à un niveau acceptable, les gestionnaires doivent alors éviter, réduire ou partager le risque.

Éviter ce risque équivaut à mettre un terme à la politique ou aux opérations qui y sont liées. Par exemple, une institution peut décider d'interdire à ses employés d'accepter de petits cadeaux de la part de partenaires de projets, ou mettre fin à sa relation avec un fournisseur à haut risque, ce qui permet d'éliminer complètement le risque. Certains risques sont inévitables, comme le risque de demandes de congés falsifiées ou le risque de demandes frauduleuses de services publics. La réduction de ces risques implique l'adaptation des procédures et des activités de contrôle afin de réduire leur probabilité et leur impact. Enfin, le partage du risque est plus courant dans le contexte des entreprises, mais il peut également être employé dans le secteur public. Il s'agit généralement de prendre des mesures pour transférer le risque à un tiers, comme une compagnie d'assurance, qui peut couvrir les pertes en cas de réalisation du risque.

Les matrices de risques, les registres de risques ou de simples tableaux Excel peuvent être des outils utiles pour documenter les résultats des évaluations de risques, ainsi que pour évaluer les liens entre les risques et les mesures de contrôle. Par exemple, le graphique 10.2, adapté du modèle d'évaluation des risques de fraude de l'Université nationale d'Australie (2017), illustre une façon de classer les notes de risque et de communiquer les actions requises, ainsi que les rôles et responsabilités des propriétaires de risques. Quelle que soit la manière dont ils sont documentés, les résultats des évaluations des risques doivent refléter le niveau de risque acceptable sur la base de critères prédéterminés. Les cartes de risques de type « cartes de chaleur »[8] ou d'autres outils permettant de noter la probabilité et l'impact des risques, sans toutefois indiquer le niveau de gestion de risques jugé acceptable par l'administration, n'ont que peu d'intérêt pour la prise de décisions ou l'adaptation de mesures d'atténuation.

Graphique 10.2. Exemple de catégories de critères de risque

Évaluation des risques	Tolérance au risque	Niveau de responsabilité	Action requise
Extrême (16-20)	Intolérable	Haut responsable	Faire remonter immédiatement aux hauts responsables et parties prenantes concernées avec un plan de traitement détaillé. Adapter les contrôles, ce qui peut inclure le renforcement des mesures existantes et l'ajout de nouvelles mesures. Assurer un suivi des risques et des contrôles de façon continue.
Élevé (11-15)	Intolérable	Directeur de programme ou chef d'équipe	Faire remonter immédiatement au cadre responsable et aux parties prenantes concernées avec un plan de traitement détaillé. Des activités de contrôles supplémentaires sont susceptibles d'être nécessaire, tant en termes de contrôles des comportements que de contrôles traditionnels. Assurer un suivi des risques et des contrôles de façon continue.
Modéré (6-10)	Acceptable	Directeur de programme ou chef d'équipe	Faire remonter immédiatement au cadre responsable avec un plan de traitement détaillé. Accroître, maintenir ou réduire les contrôles selon le score et les tendances dans l'environnement de risques. Assurer un suivi régulier des risques et des contrôles.
Faible (1-5)	Acceptable	Chargé de programme ou chargé de projet	Aucun effort de gestion n'est nécessaire. Réduire les contrôles s'ils sont considérés comme trop rigoureux et peu proportionnés aux risques. Assurer un suivi périodique des risques et des contrôles.

Source : Adapté de (Université nationale australienne, 2017[16]).

Les matrices de risque sont l'un des nombreux outils permettant un classement relatif des risques. Une organisation peut également utiliser des classements absolus, selon lesquels elle classe les risques par ordre de priorité en fonction de leurs scores numériques. Quelle que soit l'approche, les organisations doivent être conscientes des biais qui peuvent affecter le processus de notation de l'évaluation des risques, et mettre en place des processus de contrôle qualité tout au long du processus d'évaluation des risques lui-même. En effet, les cadres peuvent être incités à minimiser la perception que les activités qu'ils supervisent sont vulnérables aux risques de corruption et de fraude. Ils peuvent également exagérer les risques pour justifier des investissements plus importants dans des activités de contrôle, des outils, une formation et d'autres ressources. Les processus de validation intégrés à l'évaluation des risques peuvent contribuer à minimiser l'influence de cette partialité.

La documentation et la communication des résultats de l'évaluation des risques varieront selon les organisations ; toutefois, certaines considérations sont communes, quel que soit le contexte. Premièrement, les registres des risques, ou autres outils similaires, peuvent être utiles pour garantir l'aptitude d'une organisation à suivre les risques dans le temps, à améliorer le processus d'évaluation des risques et à renforcer les stratégies d'intégrité. Les tableaux de bord en ligne qui offrent une représentation visuelle et animée des risques peuvent également être de puissants outils pour faciliter la prise de décision en ce qui concerne les mesures d'atténuation. Deuxièmement, si une évaluation détaillée peut constituer un outil utile pour les gestionnaires et les auditeurs, dans le contexte des évaluations des risques liés à l'intégrité, elle peut également consolider des informations sensibles sur les vulnérabilités institutionnelles à la fraude et à la corruption. Dans le cadre du processus de planification de l'évaluation des risques, les

organisations peuvent envisager et communiquer explicitement les mesures de contrôle sur le processus lui-même, notamment les politiques et procédures de sécurité de l'information, l'anonymat des parties prenantes et l'utilisation des résultats. Cela peut contribuer à accroître le niveau de confort des personnes concernées et promouvoir un engagement actif dans le processus d'évaluation des risques.

10.2.3. Suivi et évaluation de la gestion des risques liés à l'intégrité

Le processus de suivi et d'évaluation est un élément clé d'un cadre global de gestion des risques qui peut aider les organisations à évaluer les politiques et les pratiques de gestion des risques liés à l'intégrité, et à y apporter les changements nécessaires. Cette activité peut être effectuée au sein du gouvernement, en se focalisant sur des questions systémiques, ou au sein d'un organe du secteur public pour améliorer la gestion des risques institutionnels.

Suivi et évaluation systémiques

L'évaluation des normes, des politiques et des procédures de contrôle interne et de gestion des risques de l'administration est une fonction essentielle pour les organisations investies de responsabilités à l'échelle du gouvernement. Ces évaluations sont souvent réalisées par des institutions d'audit interne et externe, des organes de lutte contre la corruption et des organes de réglementation, mais les institutions qui pilotent le processus peuvent varier d'un pays à l'autre. Des évaluations externes indépendantes et complètes évaluent les caractéristiques essentielles des politiques de contrôle interne et de gestion des risques, notamment la mesure dans laquelle les normes, politiques et procédures traitent des risques liés à l'intégrité, ainsi que l'harmonisation des politiques et la clarté des rôles et responsabilités dans l'environnement de contrôle pour la gestion des risques liés à l'intégrité. Par exemple, la Cour des comptes autrichienne (ACA) entreprend des audits des systèmes de prévention de la corruption des entités, qui incluent une évaluation de l'existence ou non de dispositions suffisantes pour atténuer les risques liés à l'intégrité. Ces examens peuvent révéler des lacunes à l'échelle du système, ce qui permet au gouvernement d'améliorer les cadres de contrôle interne et de gestion des risques grâce à une approche coordonnée à l'échelle du gouvernement.

Suivi et retour d'information spécifiques à l'organisation

Les changements opérationnels, réglementaires, technologiques et de nombreux autres changements peuvent influencer l'efficacité des mesures de contrôle de la fraude et de la corruption d'une organisation pour faire face aux risques. Par conséquent, les différentes mesures de contrôle interne, les activités de gestion des risques et le système de contrôle interne dans son ensemble devraient faire l'objet d'une surveillance régulière pour garantir un fonctionnement correct du cadre et des mesures de contrôle optimales. En ce sens, les activités de contrôle permettent aux organisations d'améliorer constamment les processus de gestion des risques et de contrôle : si les activités de contrôle révèlent des lacunes, les dirigeants de l'organisation peuvent superviser l'amélioration et la correction de ces lacunes en temps utile (Committee of Sponsoring Organizations of the Treadway Commission, 2016[7]). Dans le contexte de l'intégrité publique, un suivi actif du cadre de contrôle interne et de gestion des risques peut contribuer à améliorer la prévention et la détection des cas potentiels ou suspectés de fraude, de corruption ou d'abus.

Conformément à la législation ou aux politiques en vigueur, les organisations individuelles peuvent déterminer la manière dont les activités de contrôle sont menées et leur fréquence. Les évaluations continues sont des processus de routine qui permettent de suivre les activités de contrôle en temps réel, tandis que des évaluations distinctes peuvent être effectuées périodiquement par des auditeurs internes ou des parties externes. Les informations recueillies à partir des registres des risques concernant les systèmes de fraude et de corruption connus et les zones à haut risque peuvent servir de base à des activités de contrôle ciblées en appliquant une approche d'évaluation basée sur les risques.

Les institutions devraient explicitement définir les activités de contrôle et d'évaluation dans leur politique de gestion des risques liés à l'intégrité, y compris les rôles et les responsabilités. Par exemple, aux Pays-Bas, le Bureau pour la promotion de l'intégrité du secteur public (BIOS), le Bureau de l'intégrité de la municipalité d'Amsterdam et la Cour des comptes des Pays-Bas ont développé conjointement le programme IntoSAINT. Cet outil d'auto-évaluation de l'intégrité permet aux organes du secteur public d'évaluer leur vulnérabilité et leur résistance aux violations de l'intégrité, et fournit des recommandations sur la manière d'améliorer la gestion de l'intégrité. Les participants à IntoSAINT sélectionnent les processus les plus vulnérables sur la base d'un inventaire des processus primaires et de soutien de l'organisation évaluée, en identifiant les risques liés à l'intégrité les plus importants parmi ceux sélectionnés. Ces mesures sont associées à une évaluation des facteurs culturels – comme la sensibilisation et le rôle de l'administration – et de l'adéquation des mesures du système, c'est-à-dire des mesures destinées à ancrer et à consolider les politiques d'intégrité. Les résultats, qui se présentent sous la forme d'un rapport, fournissent des indications sur le fonctionnement du système d'intégrité existant. Les résultats peuvent être utilisés par les entités pour actualiser leurs politiques d'intégrité ou comme point de départ pour l'application d'autres mesures d'analyse de risque plus approfondies. La Pologne, qui a reconnu l'utilité de cet outil, a développé une auto-évaluation de l'intégrité similaire qui est distribuée aux ministères concernés.

Un autre exemple montre comment la politique de contrôle de la fraude et de la corruption du ministère de la Justice et du procureur général (DJAG) du Queensland, en Australie, attribue à un agent de contrôle de la fraude (Fraud control officer - FCO) (placé dans l'unité de gouvernance d'entreprise du ministère) la responsabilité d'améliorer activement le cadre du ministère en matière de risque de fraude et de corruption. Le FCO préside le groupe opérationnel sur le risque de fraude qui, entre autres responsabilités, surveille le cadre en supervisant les examens des politiques, les questions liées à l'audit, les plaintes, la formation et la conformité, et veille à ce que le cadre de contrôle de la fraude et de la corruption fasse l'objet d'un examen tous les deux ans ou plus fréquemment si nécessaire (Ministère de la Justice et Procureur général, 2017[17]).

10.2.4. Des procédures cohérentes et réactives dans le cadre du contrôle interne et de la gestion des risques

Le contrôle interne au sein des organes du secteur public doit comporter des procédures explicites pour répondre aux suspicions de violation de la loi, des procédures ou de manquements à l'intégrité. Bien que les mesures nécessaires puissent varier d'un organe à l'autre selon la taille, la fonction et les modalités de gouvernance, le gouvernement peut jouer un rôle essentiel dans la coordination des rapports et des réponses aux violations présumées de l'intégrité dans les organes du secteur public.

Garantir la cohérence de la réponse des organes aux manquements à l'intégrité

Un organe central peut établir des protocoles et des mécanismes normalisés pour signaler les violations présumées de l'intégrité et y répondre. Cette approche peut garantir que tous les organes du secteur public bénéficient des dispositions suffisantes pour répondre à la corruption et aux violations de l'intégrité dans le cadre de leur stratégie globale d'intégrité. Elle réduit également les doubles emplois et minimise les lacunes concernant le cadre de contrôle interne et de gestion des risques au sein des organes du secteur public. Le CdG ou un autre organe responsable peut veiller à ce que des procédures et des critères communs soient utilisés afin que les employés de l'ensemble de l'administration et le grand public puissent signaler des soupçons de violations sans crainte de représailles. Par exemple, le CdG peut élaborer des dispositions exigeant que les organes du secteur public établissent des lignes de communication séparées, comme des lignes téléphoniques dédiées. Des canaux de signalement clairs et l'existence de mécanismes de signalement cohérents sont des éléments clés d'un système de contrôle interne efficace.

Réagir aux manquements à l'intégrité au sein d'un organe

Si les politiques et les orientations fournies par le CdG favorisent la cohérence, elles ne reflètent pas toujours le contexte institutionnel de tous les organes du secteur public. En tant que tels, des mécanismes explicites peuvent aider ces organes à répondre à d'éventuels manquements à l'intégrité ou infractions légales.

Les employés sont le principal moyen de détecter ces éventuels manquements à l'intégrité ou les infractions. Les organes du secteur public peuvent créer une culture dans laquelle les employés se sentent en sécurité pour se manifester s'ils ont connaissance de manquements présumés à l'intégrité (pour en savoir plus, voir le chapitre 9). Des canaux de signalement internes et externes clairs devraient être mis en place pour les agents publics, et ces derniers devraient bénéficier d'une protection suffisante lorsqu'ils signalent des activités présumées de corruption ou de fraude. Des politiques devraient être mises en place au sein de l'organisation, pour préciser les procédures à suivre lorsqu'un employé signale un manquement présumé, et les options qui lui sont offertes. Les membres du personnel peuvent signaler les soupçons d'infraction à leurs supérieurs hiérarchiques, au personnel des ressources humaines, à l'unité d'audit interne de l'organe ou à d'autres membres du personnel désignés. De nombreux organes du secteur public ont mis en place des lignes d'assistance téléphonique pour faciliter le signalement anonyme. Quelle que soit la forme, une communication claire sur les modalités de signalement des préoccupations facilite la mise en œuvre des mécanismes de signalement.

Lorsque des soupçons de fraude ou de corruption ont été identifiés au sein d'un organe, des processus doivent être mis en place pour déclencher une réponse appropriée. Ces processus dépendront de la nature et de la gravité du comportement allégué. Par exemple, les plaintes mineures pourraient être traitées par l'administration alors que les cas plus graves, notamment si le comportement présumé peut constituer une infraction pénale, pourraient justifier une enquête approfondie. Les objectifs de toute enquête doivent être explicitement définis dans la politique d'intégrité, et ces objectifs doivent être respectés tout au long de l'enquête interne. En outre, la conformité des enquêtes à la législation en vigueur (en matière pénale et d'emploi) et avec les procédures d'enquête doit être garantie.

Une fois qu'une enquête a été entreprise, les conclusions doivent être transmises à l'administration. Les organes doivent ensuite déterminer les mesures à prendre en fonction des résultats. Si un cas de fraude ou de corruption est avéré, les mesures correctives peuvent aller de l'action disciplinaire au renvoi au pénal. Dans le cas de renvois au pénal, toute obligation de signalement externe doit être énoncée dans la politique d'intégrité de l'organisation. En outre, l'administration peut adopter une approche fondée sur les « enseignements tirés » des cas de fraude et de corruption à la suite d'une enquête.

10.2.5. Une fonction d'audit interne qui fournit une garantie et des conseils indépendants et objectifs pour renforcer le contrôle interne et la gestion des risques liés à l'intégrité

La valeur ajoutée de l'audit interne

La fonction d'audit interne examine la pertinence et l'efficacité des systèmes de contrôle interne, des procédures, des dispositifs de gouvernance, des processus de gestion des risques et de la performance des opérations des organes du secteur public (Institut des auditeurs internes, 2016[18]). Le rôle de l'audit interne devrait donc s'étendre au-delà des approches axées sur la conformité et fondées sur des règles, et inclure l'évaluation des mesures de contrôle. Cette vision contemporaine de l'audit interne saisit la valeur plus large que la fonction peut apporter à une organisation. L'audit interne peut contribuer non seulement à la réalisation des objectifs financiers et au contrôle des ressources, mais également à l'amélioration de la prise de décision et de la gestion des risques, appuyant en cela les objectifs stratégiques et opérationnels globaux.

Les auditeurs internes des organes du secteur public jouent un rôle important en fournissant des évaluations indépendantes et objectives pour déterminer si les ressources publiques sont gérées efficacement pour atteindre les résultats escomptés. Leurs connaissances et leurs preuves objectives et fondées sur des valeurs peuvent aider les organes du secteur public à mieux gérer et évaluer les risques liés à l'intégrité. Les auditeurs sont censés évaluer le potentiel de fraude et la manière dont l'organisation gère ce risque (Institut des auditeurs internes, 2016[18]). Dans la pratique, cela implique l'identification des facteurs des risques liés à l'intégrité dans le cadre du travail d'audit interne et l'évaluation de ces risques pour déterminer s'ils sont gérés efficacement, même si l'organe du secteur public ne dispose pas de programmes officiels de gestion des risques liés à l'intégrité. Par exemple, les auditeurs internes peuvent signaler les domaines à haut risque de violations en matière d'intégrité comme les relations avec des tiers, les activités externalisées ou les marchés publics. Les recommandations d'audit visant à améliorer l'environnement de contrôle dans ces domaines opérationnels à haut risque peuvent stimuler les efforts de l'organisation pour prévenir et détecter la fraude et la corruption.

Toutefois, les auditeurs internes ne sont pas censés être des enquêteurs. En fait, les mêmes normes reconnaissent que si les auditeurs internes doivent avoir des connaissances suffisantes pour évaluer les facteurs de risque de fraude et la gestion des risques de fraude au sein de l'organisation, il ne sont néanmoins pas tenus d'avoir les connaissances ou l'expertise nécessaires pour assumer un rôle d'investigation. Le rôle de l'audit interne en ce qui concerne les enquêtes sur les soupçons de manquements à l'intégrité dépend d'un certain nombre de facteurs, comme la structure de l'organisation et la disponibilité des ressources. Par exemple, l'Agence d'audit interne du gouvernement (GIAA) au Royaume-Uni offre une ligne de service distincte qui conseille les organes du secteur public sur les stratégies de lutte contre la fraude et sur la manière d'enquêter sur les soupçons de fraude interne ou de fraude à l'égard des fournisseurs. Ce service spécialisé vient s'ajouter aux activités d'audit et d'assurance internes de base fournis par le GIAA. Dans son rapport annuel pour 2018-2019, le GIAA a indiqué que le travail de l'unité de lutte contre la fraude et d'enquêtes a permis de détecter 1 million de livres sterling de fraude et d'éviter 1 million de livres sterling de pertes supplémentaires dans les organes du secteur public qui ont fait appel à ses services.

Les auditeurs internes doivent également évaluer l'efficacité des objectifs et des activités de l'organisation en matière d'éthique, ainsi que les processus de promotion de l'éthique et des valeurs. Il peut s'agir, par exemple, d'évaluer l'efficacité de la structure de gouvernance pour favoriser une culture d'intégrité ou d'auditer les processus de traitement des signalements. Des évaluations périodiques, basées sur les risques, de ces facteurs de risque d'intégrité effectuées par l'audit interne peuvent révéler les domaines les plus exposés aux manquements à l'intégrité, ce qui permet à l'administration de prendre rapidement des mesures correctives. L'Agence française anticorruption (AFA) a noté dans son enquête de 2018 sur la prévention de la corruption dans les collectivités locales que, dans certains organes du secteur public, les activités de prévention de la corruption sont explicitement incluses dans le mandat de la fonction d'audit interne.

Outre leur contribution à l'évaluation des facteurs de risque liés à l'intégrité, les auditeurs internes peuvent jouer un rôle essentiel en évaluant si les mesures de contrôle internes visant à gérer les risques liés à l'intégrité fonctionnent de manière efficace et efficiente, et en identifiant les domaines à améliorer. Cela peut prendre la forme d'un audit ou d'une évaluation de l'efficacité des composantes de la gestion des risques liés à l'intégrité, comme les programmes de lutte contre la corruption, ou d'une évaluation de la manière dont les composantes fonctionnent ensemble. La sélection d'audit basée sur le risque peut aider les auditeurs internes à déterminer la meilleure façon d'identifier les risques les plus pertinents pour les objectifs de l'organisation, et à prendre des décisions sur ce qu'il convient d'auditer en fonction de critères de risque prédéterminés. Cette approche, contrairement aux approches cycliques ou fondées sur les incidents, peut aider les auditeurs à éviter les pièges des approches axées sur la conformité et à surcharger les gestionnaires avec des audits et des mesures de contrôle.

Les résultats de l'activité d'audit interne peuvent donc aider les cadres à aligner les processus et les mesures de contrôle de gestion des risques liés à l'intégrité sur les objectifs organisationnels, de sorte que ces processus contribuent à faire progresser les objectifs stratégiques et à éclairer la prise de décision. Un certain nombre de cadres et de conseils gratuits et payants sont disponibles en ligne pour aider les auditeurs internes à évaluer les programmes d'intégrité ou de lutte contre la fraude. En général, les cadres et les orientations fournissent des indications pour les recommandations visant à améliorer à la fois les mesures de contrôle « dures » (c'est-à-dire les politiques, les procédures, la structure, etc.) et, de plus en plus, les mesures de contrôle « douces » (par exemple la culture, le comportement de l'administration, le ton au sommet), tout en reconnaissant la nécessité pour les auditeurs de prendre en compte le comportement, la motivation et les attitudes des personnes.

Les auditeurs internes peuvent jouer d'autres rôles essentiels pour promouvoir l'intégrité au sein d'un organe du secteur public. Par exemple, ils peuvent apporter une vision indépendante et objective des risques, internes et externes, pour la stratégie, l'exploitation et la réputation afin d'affiner les évaluations des risques par l'administration elle-même. En outre, la fonction d'audit interne peut être une alliée pour l'administration afin de promouvoir une culture d'intégrité. Cela comprend la participation à la sensibilisation aux risques, le renforcement des capacités (par exemple, par des formations et des ateliers), et la contribution à des messages fondés sur des valeurs concernant l'intégrité et la bonne gouvernance.

Tracer une frontière entre l'audit interne et la gestion des risques

Il est essentiel que les auditeurs internes maintiennent leur indépendance par rapport aux autres lignes de défense, qui comprennent les cadres (première ligne) et les gestionnaires de risques (deuxième ligne). Ces lignes sont souvent floues lorsqu'il s'agit de la gestion des risques liés à l'intégrité, en partie à cause des normes susmentionnées qui définissent explicitement un rôle pour l'audit interne dans l'évaluation des risques liés à l'intégrité. Toutefois, les organisations doivent veiller à ce que l'audit interne n'assume pas toutes les responsabilités relatives à la gestion des risques liés à l'intégrité. Les gestionnaires de « deuxième ligne » au sein de fonctions comme le contrôle financier, l'assurance qualité, la conformité et les unités d'inspection ont également un rôle essentiel à jouer. Par exemple, les progrès des techniques d'analyse comme les logiciels d'exploration et de couplage des données peuvent permettre aux gestionnaires des risques de surveiller les transactions financières inhabituelles qui pourraient révéler une violation en matière d'intégrité. Le tableau 10.2 suggère des moyens pour délimiter les rôles et responsabilités spécifiques des auditeurs internes afin d'éviter les doubles emplois ou les chevauchements avec d'autres lignes de défense.

Tableau 10.2. Le rôle d'un auditeur interne dans la gestion des risques liés à l'intégrité

Principaux rôles de l'audit interne	Fournir une assurance indépendante de l'efficacité et de l'efficience des processus de gestion des risques
	Évaluer les processus de gestion des risques
	Évaluer le signalement des principaux risques
	Examiner la gestion des principaux risques
	Formuler des recommandations pour améliorer la gestion des risques
Rôles d'audit interne légitimes *avec des garanties*	Faciliter l'identification et l'évaluation des risques
	Encadrer la gestion de la réponse aux risques
	Consolider les rapports sur les risques
	Développer et mettre à jour le cadre de gestion des risques
	Défendre les pratiques de gestion des risques
Rôles que l'audit interne *ne devrait pas prendre en charge*	Fixer des critères de risque
	Imposer des processus de gestion des risques
	Évaluer des risques pour les gestionnaires
	Décider de la manière d'atténuer les risques ou d'y répondre
	Mettre en œuvre des mesures d'atténuation des risques pour l'administration

Source : Adapté de (Institut des auditeurs internes, 2009[19]).

Le rôle spécifique que la fonction d'audit interne jouera en matière de gestion des risques, ou plus généralement en matière de prévention de la fraude et de la corruption, est spécifique au contexte. Le tableau 10.2 offre quelques directives relatives aux normes et aux bonnes pratiques ; cependant, dans certains pays, les lois ou les politiques offrent peu d'indications spécifiques sur le rôle de l'audit interne, ou au pire définissent un rôle qui semble en contradiction avec les normes et les bonnes pratiques internationales. Il est possible d'y remédier dans une certaine mesure au niveau institutionnel. Le rôle de l'audit interne en matière de prévention de la fraude et de la corruption, ou de gestion des risques liés à l'intégrité, doit être explicitement défini dans les politiques ou dans les documents et orientations stratégiques pertinents, comme une charte d'audit. Ce document d'orientation peut définir explicitement le rôle de l'audit interne en matière de prévention et de détection de la fraude et de la corruption, y compris l'évaluation de la gestion des risques liés à l'intégrité, la sensibilisation, les enquêtes et les rapports à l'encadrement supérieur. Comme son mandat couvre généralement les processus et les procédures de l'organisation dans son ensemble, l'audit interne est bien placé pour fournir un rapport consolidé sur la gestion des risques liés à l'intégrité au niveau institutionnel.

Les fonctions d'audit interne des organes du secteur public disposent souvent d'effectifs peu nombreux et de ressources limitées ; une coordination avec d'autres fournisseurs d'assurance sur la gestion des risques liés à l'intégrité est donc vitale. Les auditeurs peuvent s'appuyer sur le travail des fonctions de « deuxième ligne » comme les contrôleurs financiers ou les unités d'inspection, ainsi que sur celui des institutions supérieures de contrôle, des régulateurs et des médiateurs ou équivalents qui jouent également un rôle dans l'évaluation de l'efficacité des pratiques en matière de risques liés à l'intégrité. Cela peut impliquer un partage des connaissances sur une base informelle, une coordination du calendrier des activités pour minimiser l'impact sur le domaine examiné, ou des critères formels de confiance dans le travail de chacun. Au niveau gouvernemental, une approche coordonnée de la communication des informations sur la gestion des risques liés à l'intégrité peut contribuer à décloisonner les organes du secteur public, à assurer la cohérence des mesures d'atténuation des risques et à améliorer la gouvernance des risques liés à l'intégrité en général.

10.3. Défis

Les défis auxquels sont confrontés les gouvernements et les organes du secteur public diffèrent dans une certaine mesure lorsqu'il s'agit de mettre en œuvre des cadres de contrôle interne et de gestion des risques liés à l'intégrité. Les gouvernements sont à des stades de maturité différents à cet égard, et rencontrent donc des problèmes différents. Toutefois, il existe des défis communs à tous les pays. Cette section offre un aperçu de certaines des difficultés auxquelles les pays sont confrontés et des moyens qu'ils peuvent mettre en œuvre pour les surmonter, afin de mieux garantir l'intégrité. Les domaines d'intervention sont les suivants :

- combler les lacunes de mise en œuvre en s'affranchissant des approches de gestion des risques fondées sur le principe de vérification
- veiller à ce que les évaluations et les mesures de contrôle des risques s'adaptent à l'évolution de l'environnement en matière de risques
- coordonner efficacement les services répressifs et les organes d'enquête pour renforcer les boucles de rétroaction et améliorer l'évaluation des risques.

10.3.1. Combler les lacunes de mise en œuvre en s'affranchissant des approches de gestion des risques fondées sur le principe de vérification

Une approche systématique – dans laquelle la gestion des risques est explicitement liée aux objectifs organisationnels, intégrée dans les processus existants et effectuée de façon routinière – est vitale pour une gouvernance efficace des risques liés à l'intégrité dans le secteur public. Elle nécessite un fondement législatif solide accompagné de normes et de politiques qui constituent la base du contrôle interne et de la gestion des risques. Si de nombreux pays ont mis en place de telles dispositions, des lacunes persistent souvent dans la manière dont les gouvernements et les organes du secteur public mettent en œuvre les processus de gestion des risques. Par exemple, certains ont tendance à considérer les évaluations des risques comme un exercice de vérification de la conformité ou du contrôle, et, à ce titre, les effectuent sur une base ad hoc. En outre, l'encadrement supérieur et les autres employés peuvent percevoir la gestion des risques liés à l'intégrité comme une fonction qui dépasse leur rôle, s'en remettant plutôt aux auditeurs internes. Pour surmonter ces défis et renforcer les pratiques de contrôle interne et de gestion des risques au sein des entités du secteur public, les gouvernements peuvent prendre les mesures suivantes :

- *Attribuer des responsabilités explicites* – Les politiques d'intégrité peuvent attribuer des responsabilités en matière de gestion des risques de corruption, ou ces dispositions peuvent être incluses dans les politiques existantes de gestion des risques dans le cadre de l'environnement de contrôle. Conformément aux normes et modèles internationaux (par exemple, les trois lignes de défense de l'Institut des auditeurs internes), l'administration devrait être responsable de l'identification et de la gestion des risques, mais chaque employé contribue à l'efficacité de la gestion des risques au sein d'une entité. Outre les fonctions de gestion des risques, les cadres sont responsables de la gestion quotidienne des risques de fraude et de corruption – ce qui inclut la mise en place et le fonctionnement des mesures de contrôle internes – et, plus généralement, de la prévention et de la détection des risques de fraude et de corruption.
- *Renforcer les capacités par la formation* – Des programmes de formation formalisés, réguliers et continus permettent de développer les compétences et les capacités en matière de gestion des risques. Si les ressources sont limitées, les priorités en matière de formation devraient principalement cibler le personnel directement chargé d'identifier et d'atténuer les risques de fraude et de corruption. Les formateurs peuvent utiliser des enquêtes auprès des employés, des normes reconnues au niveau international et des groupes de consultation pour identifier les besoins de formation. En outre, des évaluations régulières de la formation permettent de s'assurer

que les formations du personnel prennent en considération les risques particuliers de fraude et de corruption qui se produisent dans différentes entités. Pour en savoir plus, voir le chapitre 8.

10.3.2. Veiller à ce que les évaluations et les mesures de contrôle des risques s'adaptent à l'évolution de l'environnement en matière de risques

Les risques systémiques en matière d'intégrité s'épanouissent au sein des entités qui ne procèdent pas régulièrement à des évaluations, car les activités de contrôle peuvent devenir inefficaces dans un environnement dynamique. Les mécanismes de corruption et de fraude sont en évolution constante, souvent en réponse à des changements affectant les mesures de contrôle. En outre, dans les cas les plus flagrants, un effort ponctuel de gestion et d'évaluation des risques liés à l'intégrité peut être entrepris lorsque des cadres neutralisent les mesures de contrôle et les outils de détection. Il est donc essentiel que les politiques et les cadres d'évaluation des risques liés à l'intégrité prévoient une évaluation à intervalles réguliers afin de fournir une image complète et à jour du profil de risque de l'organisation, ainsi que de l'efficacité des mesures de contrôle.

Les organisations du secteur public doivent surveiller et tester certaines mesures de contrôle, en particulier dans les domaines où les risques sont plus élevés, afin de vérifier qu'elles fonctionnent efficacement et sont proportionnelles aux risques identifiés. Étant donné que les mesures d'atténuation des risques impliquent plusieurs personnes et services différents, une communication explicite sur la manière d'évaluer l'efficacité des mesures de contrôle dans les procédures et les orientations pertinentes s'avère nécessaire. L'évaluation de la qualité des mesures de contrôle fournit des preuves de leur efficacité en matière d'atténuation des risques et devrait être communiquée à tous les responsables de risques.

10.3.3. Coordonner efficacement les services répressifs et les organes d'enquête pour renforcer les boucles de rétroaction et améliorer l'évaluation des risques

Dans les organisations du secteur public, la coordination entre les différents services et ministères est essentielle pour assurer le renvoi des cas de fraude et de corruption présumés aux services de répression et autres organes concernés. Cependant, les organisations rencontrent souvent des difficultés pour assurer le suivi auprès des autorités concernant l'issue des incidents de fraude et de corruption signalés. Le manque de communication autour des affaires ayant fait l'objet de poursuites représente un défi important pour les entités lorsqu'elles évaluent leurs mesures de contrôle et prennent des mesures correctives.

L'amélioration des boucles de rétroaction concernant les poursuites et les corrections peut améliorer l'évaluation des risques, renforcer la dissuasion de la fraude et de la corruption et permettre aux organisations de s'attaquer plus efficacement aux lacunes de leurs dispositifs de contrôle, réduisant ainsi le risque que des incidents similaires se produisent à l'avenir. Un moyen d'y parvenir consiste à mettre en place des ateliers d'échange d'informations avec la participation des services de répression et des organes d'enquête, afin d'aider les organisations à identifier les tendances, les modèles et les modes opératoires en matière de fraude et de corruption.

Références

Bureau de la gestion et du budget fédéraux (2016), *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk*, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf. [5]

Bureau gouvernemental des comptes (2015), *A Framework for Managing Fraud Risks in Federal Programs*, https://www.gao.gov/assets/680/671664.pdf. [4]

Bureau gouvernemental des comptes (2014), *Standards for Internal Control in the Federal Government*, https://www.gao.gov/assets/670/665712.pdf. [3]

Commission européenne (2015), *Public Internal Control Systems in the European Union*, https://ec.europa.eu/budget/pic/lib/docs/2015/CD02PrinciplesofPIC-PositionPaper.pdf. [6]

Committee of Sponsoring Organizations of the Treadway Commission (2016), *Fraud Risk Management Guide*, https://www.coso.org/Pages/Purchase-Guide.aspx (consulté le 17 février 2020). [7]

Committee of Sponsoring Organizations of the Treadway Commission (2013), *Internal Control - Integrated Framework*, https://www.coso.org/Pages/ic.aspx (consulté le 17 février 2020). [2]

Crime and Corruption Commission (2018), *Fraud and Corruption Control - Best Practice Guide*, https://www.ccc.qld.gov.au/publications/fraud-and-corruption-control-best-practice-guide (consulté le 17 février 2020). [9]

Fountain, L. (2015), *Raise the Red Flag: An Internal Auditor's Guide to Detect and Prevent Fraud*, The Institute of Internal Auditors Research Foundation. [15]

Institut des auditeurs internes (2016), *International Professional Practices Framework (IPPF) – Standards and Guidance*, https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx. [18]

Institut des auditeurs internes (2009), *The Role of Internal Auditing in Enterprise-Wide Risk Management*, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf. [19]

Irish Health Service Executive (2018), *Risk Management Support Tools*, https://www.hse.ie/eng/about/qavd/riskmanagement/risk-management-documentation/risk%20management%20support%20tools%20.html (consulté le 17 février 2020). [11]

Ministère de la Justice estonien (2013), *Anti-Corruption Strategy 2013-2020*, https://www.korruptsioon.ee/en/anti-corruption-activity/anti-corruption-strategy-2013-2020 (consulté le 24 janvier 2020). [8]

Ministère de la Justice et Procureur général (2017), *Fraud and corruption control policy*, https://www.justice.qld.gov.au/__data/assets/pdf_file/0020/534350/fraud-and-corruption-control-policy.pdf. [17]

National Audit Office (2011), *Managing risks in government*, https://www.nao.org.uk/report/managing-risks-in-government/ (consulté le 17 février 2020). [13]

OCDE (2017), *Recommandation du Conseil sur l'intégrité publique*, OCDE, Paris, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0435 (consulté le 24 janvier 2020). [1]

OCDE (2015), *Prevention of Corruption in the Public Sector in Eastern Europe and Central Asia*, OECD Anti-Corruption Network for Eastern Europe and Central Asia, OCDE, Paris, http://www.oecd.org/investment/anti-bribery/ACN-Prevention-Corruption-Report.pdf. [12]

Organisation internationale de la normalisation (2018), *ISO 31000:2018, Risk Management - Guidelines*, https://www.iso.org/iso-31000-risk-management.html. [10]

Université nationale australienne (2017), *Fraud Risk Assessment Template*, https://services.anu.edu.au/planning-governance/risk-audit/fraud-prevention-and-control (consulté le 17 février 2020). [16]

Wright Jr., R. (2013), *The Internal Auditors' Guide to Risk Assessment*, The Institute of Internal Auditors Research Foundation. [14]

Notes

[1] L'environnement de contrôle est constitué d'un ensemble de normes, de processus et de structures qui constituent la base du contrôle interne dans une organisation.

[2] Dans le modèle des trois lignes de défense, la première ligne de défense comprend les cadres opérationnels qui s'approprient et gèrent les risques. La deuxième ligne de défense comprend les fonctions de supervision des risques, généralement des fonctions de gestion des risques et de conformité. La troisième ligne de défense comprend les fonctions d'audit interne qui fournissent une assurance indépendante de l'efficacité des processus de gestion des risques.

[3] Les risques inhérents sont des risques évalués en l'absence de mesures de contrôle, c'est-à-dire avant l'application des mesures de contrôle.

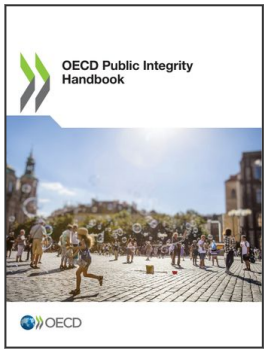
[4] Le risque résiduel est le niveau de risque restant après application des mesures d'atténuation.

[5] Les risques stratégiques sont la probabilité qu'il se produise un événement susceptible d'affecter la capacité d'une organisation à atteindre les objectifs escomptés. Les risques opérationnels sont la probabilité que se produise un événement qui affectera la capacité d'une organisation à atteindre ses objectifs et à produire des résultats. Les risques pour la réputation font référence au potentiel de publicité négative, de perception publique ou d'événements incontrôlables ayant un impact négatif sur la réputation d'une organisation.

[6] Les facteurs de risque sont des caractéristiques de l'environnement, des politiques, des procédures ou des activités d'une organisation qui sont associées à un risque élevé.

[7] La tolérance aux risques correspond au niveau de risque que les gestionnaires sont prêts à accepter après avoir mis en œuvre des activités de contrôle. La définition de la tolérance aux risques permet de guider les agents publics dans leurs décisions d'accepter, de réduire, d'éviter ou de partager les risques.

[8] Une carte thermique est une représentation des évaluations quantitatives et qualitatives de la probabilité d'occurrence d'un risque et de son impact sur l'organisation si ce risque particulier venait à se produire.



Extrait de :

OECD Public Integrity Handbook

Accéder à cette publication :
https://doi.org/10.1787/ac8ed8e8-en

Merci de citer ce chapitre comme suit :

OCDE (2020), « Gestion des risques », dans *OECD Public Integrity Handbook*, Éditions OCDE, Paris.

DOI: https://doi.org/10.1787/20cf6c56-fr