LA GESTION DES RISQUES À L'INTÉGRITÉ

POUR LES ORGANISATIONS PUBLIQUES

ENSEMBLE on fait avancer le Québec

Québec

LA GESTION DES RISQUES À L'INTÉGRITÉ

POUR LES ORGANISATIONS PUBLIQUES

Cette publication a été réalisée conjointement par la
Direction de la prévention et des communications
de l'Unité permanente anticorruption et la
Direction du développement des personnes et des organisations
du Secrétariat du Conseil du trésor
en collaboration avec sa Direction des communications.

Direction du développement des personnes et des organisations
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8
Téléphone : 418 643-0875, poste 4666

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant le site Internet du Conseil.

Direction des communications
Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
Site Internet : www.tresor.gouv.qc.ca

Dépôt légal – juin 2016
Bibliothèque et Archives nationales du Québec
ISBN 978-2-550-76145-7 (en ligne)

TABLE DES MATIÈRES

REMERCIEMENTS

Le Secrétariat du Conseil du trésor (SCT) et l'Unité permanente anticorruption (UPAC) tiennent à reconnaître tous les efforts déployés pour l'élaboration du présent document sur la gestion des risques à l'intégrité pour les organisations publiques.

Le document a été inspiré des travaux de :

Jacques Beaupré, directeur de la prévention et des communications de l'UPAC,

Farid Al Mahsani, conseiller expert en gestion des risques du SCT et de l'UPAC,

Denis Thiffault, coordonnateur gouvernemental en éthique pour la fonction publique, au Secrétariat du Conseil du trésor

Normand Julien, Magalie Jutras et Hugo Roy, membres de l'équipe de travail de la Direction des services aux organisations de l'École nationale d'administration publique, et

Marie-France Lebouc, professeure à la Faculté des sciences de l'administration de l'Université Laval.

Rédaction finale : Denis Thiffault et Jacques Beaupré

Nos remerciements s'adressent à ces personnes pour l'engagement et l'énergie dont elles ont fait preuve, deux facteurs essentiels à la réussite du projet.

MESSAGE

En matière de saine gouvernance, la gestion des risques constitue un outil préventif qui permet aux organisations publiques d'identifier et de gérer adéquatement certaines situations auxquelles elles doivent faire face dans la conduite de leurs affaires. Plus précisément, la gestion des risques à l'intégrité agit comme un instrument fondamental de planification organisationnelle en matière d'intégrité.

Le document La gestion des risques à l'intégrité pour les organisations publiques est issu de la collaboration de la Direction de la prévention et des communications de l'Unité permanente anticorruption et de la Direction du développement des personnes et des organisations pour la fonction publique québécoise, au Secrétariat du Conseil du trésor. Il combine la prévention et la gestion des risques organisationnels en matière d'éthique ainsi que des risques à la corruption et à d'autres actes répréhensibles.

Le processus de gestion des risques à l'intégrité suggéré se veut une démarche dynamique et intégrée à la mission, aux valeurs et aux processus organisationnels.

Ce document propose aux organisations une démarche simple, basée sur les meilleures pratiques tout en présentant des définitions opérantes de l'intégrité, de l'éthique, de la corruption et des risques inhérents. Finalement, il constitue une invitation aux organisations publiques à commencer ou à poursuivre l'examen de leurs principaux risques et des mesures mises en place pour les contrôler.

INTRODUCTION

La notoriété accordée par les Québécoises et les Québécois aux organisations publiques résulte de l'effet combiné de l'image projetée par ces dernières et de la réputation favorable ou défavorable qu'on leur attribue. La démarche de gestion des risques, ici proposée, doit, d'abord et avant tout, servir à maintenir et à consolider la confiance des citoyens à l'endroit de l'intégrité de leurs organisations publiques.

Le présent document propose aux organisations publiques une stratégie, une démarche et des outils leur permettant de gérer les risques prévisibles en matière d'intégrité, tout en les aidant à élaborer un plan de gestion de ces risques.

L'approche préconisée se base sur une démarche méthodique simple de gestion des risques. La stratégie s'appuie sur les travaux du Secrétariat du Conseil du trésor (SCT), du Commissaire à la lutte contre la corruption et de l'École nationale d'administration publique (ENAP) ; elle s'inspire en outre des normes de qualité des pratiques généralement reconnues à l'échelle internationale[1].

La première partie du document s'adresse principalement aux décideurs des organisations publiques. Elle propose une définition de l'intégrité et de ses risques inhérents. Ces risques se déclinent en deux types distincts, soit les risques de nature éthique et les risques liés à la corruption et aux autres actes répréhensibles. De plus, cette partie vise à favoriser la prise de décision quant à la mise en place d'un processus de gestion des risques, tout en présentant ses préalables et ses conditions de succès. La stratégie suggérée poursuit l'objectif prioritaire d'identifier ces types de risques et de permettre à l'organisation d'agir adéquatement pour contrer ces derniers afin d'en atténuer les préjudices potentiels.

La seconde partie du document s'adresse plus particulièrement aux responsables de la démarche en présentant une méthode de travail et en suggérant des outils pour réaliser leur mandat.

Les outils annexés permettent de réaliser une représentation claire des risques, mais, aussi, de bien saisir la nature de chaque risque identifié et d'en apprécier les répercussions sur l'organisation.

Le processus de gestion des risques suggéré peut être adapté selon les besoins particuliers, la mission ou la taille de l'organisation, ou s'intégrer à un processus de gestion des risques déjà existant.

Certaines organisations ont déjà une expertise et une démarche structurée de gestion des risques. Cependant, peu d'entre elles incluent les risques à l'intégrité dans leurs facteurs d'analyse. Pour ces organisations, l'objectif sera donc d'ajouter l'analyse de ces risques à ceux déjà évalués et d'assurer la mise en place des mesures d'atténuation appropriées afin de réduire ou d'annuler leurs effets indésirables.

À l'échelle gouvernementale, la démarche de gestion des risques à l'intégrité trouve ses fondements dans le document Attentes gouvernementales 2016-2017 – au point 1 : « Développer une véritable culture d'intégrité, de transparence et d'écoute en faisant preuve de probité et en traitant avec célérité les questions touchant l'intégrité et l'éthique des institutions publiques et des individus, en portant une attention particulière à l'intégrité des processus de gestion contractuelle, et en mettant à la disposition de la population l'information nécessaire lui permettant de s'informer, d'engager le dialogue et de réagir à certaines initiatives. »

En introduction à son document intitulé Politique-cadre de gestion des ressources humaines, le Secrétariat du Conseil du trésor précise que : « […] l'efficacité et l'efficience de la prestation de services, la rigueur et la transparence dans l'utilisation des fonds publics, le maintien et le développement de l'expertise de la fonction publique, la flexibilité dans les façons de faire et enfin le renforcement d'une culture d'intégrité constituent les défis majeurs que la fonction publique doit impérativement relever. » Plus précisément, on présente dans la politique-cadre l'énoncé suivant : « Au regard des nouveaux enjeux découlant de l'évolution du contexte social, économique et technologique, le Conseil du trésor réaffirme et renforce le respect des valeurs de la fonction publique, notamment en ce qui touche l'éthique et la déontologie. »

---

1 ISO 31000 : 2009 ; Guide ISO 73 : 2009 ; *Project Management Institute* (PMI) et le document intitulé Vers un cadre pour l'intégrité solide : instruments, processus, structures et conditions de mise en œuvre de l'Organisation de coopération et de développement économiques (OCDE).

Cette démarche s'inscrit également dans la réalisation des mandats confiés au Commissaire à la lutte contre la corruption et à l'Unité permanente anticorruption (UPAC), qui doivent assumer un rôle de prévention et d'éducation en matière de lutte à la corruption, comme le prévoit l'article 9 de la Loi concernant la lutte contre la corruption :

« 9. Le commissaire a pour fonctions :

[…]

6° d'assumer un rôle de prévention et d'éducation en matière de lutte contre la corruption.

Le commissaire peut en outre effectuer ou faire effectuer toute enquête ou tout complément d'enquête à la demande du directeur des poursuites criminelles et pénales.

Le commissaire exerce également toute autre fonction que lui confie le gouvernement ou le ministre. »

PARTIE 1

1.1 MISE EN CONTEXTE

Afin de demeurer à la fine pointe des développements et de poursuivre l'amélioration continue de leurs pratiques de gestion, les organisations publiques s'inspirent des meilleures pratiques à l'échelle internationale dans le domaine de la gestion intégrée des risques. Si les démarches en matière d'identification des risques à l'intégrité sont relativement nouvelles, cela ne signifie pas pour autant que le Québec soit le seul État qui ait décidé de s'y attaquer.

Depuis plus d'une décennie, l'Organisation de Coopération et Développement Économiques (OCDE), regroupant 34 pays membres, accumule des données et une expertise en matière de gouvernance, d'éthique et d'intégrité. Pionnière dans le domaine de l'intégrité publique, elle a effectué plusieurs évaluations comparatives permettant de reconnaître les meilleures pratiques organisationnelles et gouvernementales dans le domaine.

En 2009, la publication du document de l'OCDE, intitulé Vers un cadre pour l'intégrité solide : instruments, processus, structures et conditions de mise en œuvre, est venue consolider l'approche d'éthique préventive que cette organisation propose. Cette approche reconnaît l'importance, pour les administrations publiques modernes comme celle du Québec, de travailler en amont de ces risques, permettant ainsi d'éviter les dérapages et favorisant une gestion préventive de ceux-ci. Reconnue pour son leadership en matière d'intégrité, l'OCDE recommande aux administrations publiques de bien s'outiller en matière d'éthique préventive et leur propose de se doter d'une rigoureuse cartographie des risques auxquels elles sont exposées.

L'un des principes de base de l'approche de l'OCDE est de considérer les risques à l'intégrité non pas isolément, mais de façon globale. Ainsi, les risques à l'intégrité ne sont pas réduits à quelques mauvaises actions ou à la négligence de quelques personnes. Ces risques résultent de processus organisationnels systémiques et récurrents que seul un exercice minutieux d'identification et d'évaluation peut cerner de manière efficace. Cette stratégie d'identification globale permet ainsi aux décideurs de mieux saisir les récurrences de certains risques d'intégrité, de mieux les comprendre et, ainsi, de s'y attaquer à la source.

Divers facteurs expliquent en quoi un processus de gestion des risques à l'intégrité est devenu incontournable. Nous mentionnerons brièvement ici les plus importants :

- La poursuite de l'intérêt général constitue la mission fondamentale des organisations publiques. Ces mêmes organisations sont au service de l'ensemble des citoyens. Ce constat impose au personnel de ces organisations le respect rigoureux de règles de conduite et des lois.
- Les questionnements et les exigences de la population ainsi que les enquêtes journalistiques en matière d'intégrité exercent une pression sur les organisations publiques pour que celles-ci maintiennent et améliorent leur performance et leur leadership en matière d'intégrité.
- D'une part, la Loi sur l'administration publique privilégie la qualité des services aux citoyens, un cadre de gestion axé sur les résultats et le respect du principe de transparence. D'autre part, les dirigeants d'organisations publiques sont imputables de leur gestion devant les parlementaires qui leur confient, entre autres, les mandats suivants :
  - prise en charge des attentes de la population en fonction des ressources disponibles ;
  - atteinte de résultats en fonction d'objectifs préalablement établis et d'une reddition de comptes crédible et fiable sur l'atteinte de ces mêmes résultats ;
  - flexibilité des organisations publiques en ce qui a trait à l'adaptation de leurs règles de gestion à leur situation.
- Dans le but de répondre aux besoins des citoyens, les organisations publiques québécoises font parfois appel au secteur privé dans divers domaines. Ce contact accru entre des organisations privées, ayant pour objectif la recherche du profit, et le secteur public, mandataire de l'intérêt général, soulève parfois des questionnements

sur les pratiques ayant cours dans le secteur public. Dans de telles circonstances, les frontières entre le secteur public et le secteur privé deviennent parfois imprécises, tout en créant des zones de risques potentiels.

- Les organisations publiques sont également exposées aux changements rapides que vit le monde du travail. Le personnel des organisations publiques évolue à la fois dans des zones grises et dans un cadre normatif de plus en plus complexe et spécialisé. De plus, la mobilité du personnel et son rythme de renouvellement, les nombreux départs à la retraite, les distinctions générationnelles et culturelles, la multiplication des partenaires et la sous-traitance constituent des facteurs qui rendent plus complexe le rôle du personnel des organisations publiques. L'environnement de travail ouvre ainsi la porte à des risques à l'intégrité[2].
- Les administrations publiques contemporaines exigent que les questions d'intégrité dépassent le simple effet de mode ou la logique des scandales. L'intégrité constitue un des enjeux primordiaux pour l'administration publique québécoise, comme pour tous les États modernes. L'efficience, la transparence, la saine gestion des fonds publics, le sens de l'État ainsi que l'intégrité des personnes, de leurs fonctions, des processus et des organisations sont des incontournables pour l'État moderne.

À la lumière de ce qui précède, les modes de fonctionnement des administrations publiques se transforment. Le processus de gestion des risques à l'intégrité peut servir d'outil pour aider les organisations publiques québécoises et leur personnel à s'adapter à ces nouvelles réalités, ce qui leur permettra de consolider le niveau de confiance des citoyens envers leurs institutions et la notoriété de ces dernières.

1.2 L'INTÉGRITÉ ET LE RISQUE À L'INTÉGRITÉ

Aux fins du processus de gestion des risques proposé, il est essentiel de définir le type de risques à identifier.

La Déclaration des valeurs de l'administration publique québécoise présente l'intégrité sous la forme de normes comportementales : « Chaque membre de l'administration publique se conduit d'une manière juste et honnête. Il évite de se mettre dans une situation où il se rendrait redevable à quiconque pourrait l'influencer indûment dans l'exercice de ses fonctions. »

La définition de la valeur d'intégrité pour les organisations publiques doit être consensuelle, dynamique et actualisée.

> L'intégrité est une valeur fondamentale qui soutient de manière continue et cohérente les décisions, les actions et les comportements d'une personne. L'intégrité en milieu de travail s'actualise par l'adéquation des décisions, des actions et des conduites à des valeurs telles l'honnêteté, la probité, le respect, la loyauté, la compétence, l'équité, l'impartialité et la transparence.

Concrètement, pour les organisations publiques, les décisions et les actions d'une personne intègre se traduisent par des conduites fidèles à la mission de l'organisation, au système de valeurs en place et aux cadres déontologique, légal et réglementaire applicables.

Les membres du personnel des organisations publiques et leurs partenaires sont appelés à mettre en place et à opérer divers processus visant ultimement la poursuite du bien public. Ces processus se doivent d'être intègres.

La synergie d'intégrité ainsi créée par la combinaison des actions des membres du personnel, dans le cadre de leurs fonctions professionnelles, sur les processus de l'organisation participe activement à la culture organisationnelle d'intégrité.

2 MICHAUD, Nelson et al. Secrets d'États? Les principes qui guident l'administration publique et ses enjeux contemporains, 2011, 810 p.

Le risque à l'intégrité

Nous souscrivons à la définition suivante du risque comme étant : « l'effet de l'incertitude sur l'atteinte des objectifs.[3] » Il se mesure par le produit de la probabilité et des impacts d'un événement. Il permet de qualifier une situation et d'agir en conséquence[4].

Plus précisément et afin de nous assurer d'un langage commun et opératoire en matière de gestion des risques à l'intégrité, nous proposons les définitions suivantes :

Le risque à l'intégrité est une **situation** menaçant l'**actualisation** de la mission, des valeurs, des règles déontologiques et des dispositions légales de l'organisation, pouvant causer **préjudice** à une ou des parties prenantes.

Situation : Une situation peut être une action, une inaction, une décision, une indécision, des paroles ou des comportements.

Actualisation : L'actualisation des règles, des valeurs organisationnelles et des valeurs de l'administration publique signifie le passage des règles et des valeurs affichées vers des valeurs vécues, vers des valeurs et règles prônées et vers des actions concrètes et quotidiennes (passage du discours à l'acte, de la parole aux gestes).

Préjudice : Atteinte aux droits, aux intérêts et au bien-être d'une partie prenante ou d'un État.

Plusieurs facteurs peuvent donner naissance à ces situations ; nous en notons ici quelques-uns. Il s'agit, par exemple, de situations où il y a :

- absence totale de règles ou de normes ;
- des normes et des règles inadéquates ou désuètes ;
- des règles méconnues ou incomprises ;
- des normes et des règles laissant place à une interprétation trop large ou créant de la confusion ;
- plusieurs normes ou valeurs entrant en conflit ;
- existence de règles ou de normes claires, mais faisant l'objet d'une surveillance défaillante ou absente ;
- des intérêts, financiers ou autres, qu'ils soient directs ou indirects, réels ou apparents, effectifs ou potentiels (p. ex., conflits d'intérêts).

Les risques à l'intégrité se déclinent en deux types distincts, soit les risques de nature éthique et les risques liés à la corruption et à d'autres actes répréhensibles.

3 ISO 31000 : 2009 ; Guide ISO 73 : 2009 ; *Project Management Institute* (PMI) et le document intitulé Vers un cadre pour l'intégrité solide : instruments, processus, structures et conditions de mise en œuvre de l'Organisation de coopération et de développement économiques (OCDE).

4 TAYLOR-GOOBY, Peter et Jens O. ZINN. *Risk in Social Science*, Oxford University Press, 2006, p. 22-26.

1.3 L'ÉTHIQUE ET LE RISQUE ÉTHIQUE

Nous définissons l'éthique comme étant un mode de régulation des comportements qui provient du jugement personnel et des valeurs d'une personne, en se fondant sur la mission et les valeurs partagées par l'organisation dont elle fait partie.

Le risque éthique

La gestion du risque éthique s'attardera de manière préventive au respect de la mission de l'organisation et à l'actualisation de ses valeurs.

> Les risques en matière d'éthique représentent des situations de « zones grises » où les possibilités de conduites à adopter sont multiples et où les opportunités de manquements sont les plus susceptibles de survenir. Les organisations sont exposées à des risques en matière d'éthique lorsqu'une ou plusieurs personnes ont la possibilité d'adopter des comportements qui ne peuvent se justifier à la lumière des valeurs partagées au sein de l'organisation, ou qui mettent en péril la mission de l'organisation, tout en pouvant causer des préjudices aux parties prenantes.

En général, ces risques peuvent :

- être connus du personnel de l'organisation et être déjà bien encadrés (p. ex., processus de dotation);
- être connus de l'organisation, mais ignorés des membres de son personnel (p. ex., une nouvelle directive sur la disposition et la destruction des documents contenant des informations confidentielles);
- être méconnus du personnel de l'organisation (p. ex., utilisation des médias sociaux).

Ces risques peuvent être présents dans plusieurs types de processus de l'organisation, telles la gestion des ressources humaines, la gouvernance, l'acquisition des biens et services, les relations avec les parties prenantes, etc.

1.4 LA CORRUPTION ET LE RISQUE À LA CORRUPTION

CORRUPTION = monopole + pouvoir discrétionnaire – transparence

KLITGAARD, Robert, économiste, professeur à Claremont Graduate University et expert en matière de lutte contre la corruption

La corruption est multiforme et insidieuse. Elle peut s'immiscer dans toutes les activités d'une organisation. Il existe autant de définitions de la corruption que de manifestations de cette dernière. Ces manifestations peuvent se traduire par de nombreux actes répréhensibles. Préalablement à une définition commune et utile aux fins de la gestion des risques à l'intégrité, nous devons examiner soigneusement le concept de corruption.

Pour une organisation publique, la corruption constitue une confrontation entre sa mission première, soit la poursuite de l'intérêt public, et la recherche d'avantages indus de la part d'intérêts tiers.

La corruption peut s'installer au sein d'une organisation publique lorsqu'une personne, dans l'exercice de ses fonctions, peu importe sa position dans l'organisation, bénéficie d'un pouvoir discrétionnaire pouvant conférer des avantages indus à d'autres intérêts.

Plus précisément, il y a corruption dans une organisation publique :

- lorsqu'une personne d'une organisation publique (le « corrompu »)
- sollicite ou accepte, directement ou indirectement, immédiatement ou pour le futur,
- une gratification, une faveur, une somme d'argent, une récompense ou tout autre avantage sous quelque forme que ce soit
- pour lui-même ou des proches
- en échangeant ou tentant d'échanger
- l'exercice abusif de son pouvoir discrétionnaire ou l'omission dans l'application de règles
- aux fins de l'obtention d'un avantage indu, en matière, notamment, d'obtention de contrats publics d'acquisition de biens et services, de subventions, de permis, d'accès privilégiés à des services publics, d'une charge, d'un emploi ou d'information privilégiée de nature confidentielle
- par un intérêt tiers (le « corrupteur »).

Concrètement :

- Pour le « corrompu », la corruption se matérialise par la sollicitation ou l'acceptation, réelle ou non, d'un don ou de toute offre d'avantages faite par un « corrupteur » en échange d'une action, d'une inaction ou d'une abstention d'agir, conférant ainsi un avantage indu au « corrupteur ».
- Pour le « corrupteur », la corruption se matérialise par l'offre, acceptée ou non, d'un don ou de toute offre d'avantages à l'intention d'un « corrompu » en échange de son action, inaction ou abstention d'agir, en vue d'obtenir un avantage indu.

Les actes répréhensibles

Lorsque la corruption tente de s'installer dans une organisation publique, elle peut se manifester sous plusieurs formes, que nous appellerons les actes répréhensibles, et qui peuvent être, notamment :

- une contravention aux dispositions des lois et des règlements en vigueur au Québec et au Canada, entre autres :
  - la malversation,
  - la collusion,
  - la fraude,
  - le trafic d'influence,
  - le pot-de-vin,
  - l'abus de confiance,
  - etc.
- l'usage abusif de fonds ou de biens publics ;
- le fait d'ordonner ou de conseiller à une personne de commettre un acte répréhensible.

Le risque à la corruption

La gestion du risque à la corruption s'attardera de manière préventive au respect rigoureux des règles applicables dans les processus et activités de l'organisation publique.

Les risques en matière de corruption représentent des situations de « zones grises » où les possibilités de conduites à adopter sont multiples et où les opportunités de manquements sont les plus susceptibles de survenir. Les organisations sont exposées à des risques de corruption lorsqu'une ou plusieurs personnes ont la possibilité d'exercer un pouvoir décisionnel discrétionnaire ne pouvant se justifier à la lumière des règles, normes, politiques et lois applicables à l'organisation, et qui met en péril la mission de service public de l'organisation, tout en pouvant causer des préjudices aux parties prenantes.

1.5 LES OBJECTIFS POURSUIVIS ET LA VALEUR AJOUTÉE

Rappelons que, pour les organisations publiques, la gestion des risques à l'intégrité permettra de cibler de manière proactive les risques les plus importants auxquels elles sont exposées et les facteurs d'incertitude associés. Cette démarche favorisera aussi la mise en place de mesures et de plans d'action utiles à l'atténuation des risques et au renforcement de la confiance de la population à l'endroit des organisations publiques et des services qu'elles offrent.

Pour le personnel des organisations publiques, une démarche participative de gestion des risques à l'intégrité constitue l'occasion de collaborer à l'amélioration continue des pratiques de l'organisation. Les membres du personnel seront encouragés à réagir aux risques liés aux changements ou aux nouvelles pratiques. De plus, comme la gestion des risques est un processus à la fois itératif et réactif aux changements à intégrer aux pratiques organisationnelles, le personnel des organisations publiques sera régulièrement interpellé et sensibilisé aux questions d'intégrité.

Généralement, le personnel dispose de l'information nécessaire à l'identification et à l'analyse des risques. Le personnel possède aussi l'expérience pour décider et agir dans l'incertitude. En associant les membres du personnel à la démarche de gestion des risques à l'intégrité, ceux-ci deviennent des parties prenantes et peuvent contribuer activement à la consolidation de la culture d'intégrité de l'organisation.

En dernier lieu, la gestion des risques à l'intégrité permet aux organisations et aux parties prenantes de minimiser, de manière proactive, les dérapages éthiques, les actes répréhensibles, les situations préjudiciables et les coûts qui leur sont associés.

1.6 LES CONDITIONS DE SUCCÈS DE LA DÉMARCHE

Le succès du processus de gestion des risques repose sur certains éléments fondamentaux. La présence ou la mise en place de ces éléments donneront à la haute direction l'assurance raisonnable et continue que l'environnement dans lequel évolue l'organisation est propice au développement d'une culture d'intégrité.

1.6.1 Un leadership éclairé et une vision de la haute direction

La recherche de l'intégrité par la gestion des risques incombe avant tout aux instances de l'organisation. Le leadership de la haute direction est un élément clé de la mise en œuvre et de l'amélioration continue en matière de gestion des risques à l'intégrité. L'actualisation de la valeur d'intégrité et des valeurs sous-jacentes véhiculées par les instances organisationnelles se doit d'être tournée vers l'intégrité des personnes, de leurs fonctions, des processus et de l'organisation. Cette vision doit être partagée par tous les membres de l'organisation sous la forme d'un consensus organisationnel auquel adhèrent toutes les parties prenantes.

La manière dont les gestionnaires de niveau supérieur décident et agissent influence directement la culture organisationnelle d'intégrité. Il en va de même pour ce qui est de leurs comportements et de leurs efforts pour assurer la mise en place, le fonctionnement et la mise à jour du plan de prévention des risques à l'intégrité.

1.6.2 Une culture organisationnelle d'intégrité

La culture organisationnelle influe sur la façon de prendre les décisions et d'agir dans une organisation. C'est par l'actualisation des valeurs que la culture d'intégrité se développe et ces mêmes valeurs, en plus d'être affichées, se doivent d'être partagées. Si la culture de l'organisation accepte, ignore ou banalise les actes répréhensibles, il y a de fortes probabilités que ceux-ci s'installent et se répandent. Par contre, si la culture organisationnelle encourage et reconnaît les comportements qui sont conformes à une stratégie de sensibilisation à la corruption et aux manquements éthiques et de lutte contre ces derniers, les probabilités de matérialisation des actes répréhensibles à l'intérieur de l'organisation seront d'autant réduites. Les gestionnaires occupant une position d'influence peuvent favoriser le maintien et la consolidation d'une véritable culture d'intégrité, en encourageant les comportements conformes, le soutien au personnel et les contrôles inhérents.

1.6.3 Un groupe de travail multidisciplinaire diversifié

Pour réaliser le mandat d'identification et d'évaluation des risques, il est recommandé que chaque organisation se dote d'un groupe de travail multidisciplinaire. Ce groupe permettra de mieux saisir les différentes représentations que l'organisation peut se faire du risque. Il permettra aussi de proposer les changements favorables à l'implantation d'une culture d'intégrité organisationnelle. Les organisations disposant déjà d'un comité de coordination et de gestion des risques peuvent l'utiliser comme groupe de travail. Ce groupe de travail pourrait être permanent et se charger du suivi de la gestion des risques liés à l'intégrité.

Certains facteurs seront déterminants dans le choix des membres de l'organisation qui y participeront. La gestion des risques est un processus qui exige une très grande collaboration des participants, ainsi qu'une coordination et une complémentarité avec les autres intervenants de l'organisation (gestion intégrée des risques, audit interne, sécurité de l'information, gestion de projet, répondants en éthique, etc.). La taille de l'organisation, son contexte d'opération, sa mission, son historique, ses ressources et ses standards en matière d'intégrité sont autant d'éléments qui doivent guider les instances dans leurs choix. Les membres de ce groupe de travail connaîtront les bases et les principes fondamentaux d'un exercice de gestion des risques, les objectifs poursuivis et les implications qui en découlent, tant pour eux que pour l'organisation. Ils s'assureront, en outre, d'avoir une compréhension commune de la démarche de gestion des risques à l'intégrité. Ils seront également invités à utiliser le même langage pour y référer, afin d'assurer un message cohérent et constant à l'ensemble des membres de l'organisation.

1.6.4 Un plan de travail efficace

Il faut également s'assurer que les personnes chargées de réaliser la démarche disposent d'un plan de travail efficace. L'effort consenti pour la planification et le temps investi pour la sensibilisation des participants à la démarche sont autant de conditions gagnantes pour la réussite de l'opération dans les délais impartis.

1.6.5 Un plan de communication efficace

Le succès de la démarche est également tributaire de l'efficacité de la communication et de la consultation avec les différents acteurs. Un plan de communication interne et externe doit permettre de définir le contexte des risques de manière appropriée, d'assurer la bonne compréhension et la prise en compte des intérêts des parties prenantes, y compris ceux des membres du personnel, ainsi que de rassembler différentes expertises permettant d'identifier, d'analyser et d'évaluer adéquatement les risques et leurs conséquences.

1.6.6 Un état de situation sur les systèmes et les politiques de gestion de l'organisation

L'organisation publique désireuse de consolider et de développer sa culture d'intégrité en menant un exercice de gestion des risques s'assurera de la disponibilité et de la maîtrise de certains systèmes. Elle doit, au cours du processus, être en mesure de les recenser, de les examiner et de s'assurer de leur appropriation par les parties prenantes.

Un système d'éthique organisationnelle

Les organisations publiques désirant parer les comportements déviants doivent minimalement disposer des éléments appropriés, soit :

- une déclaration des valeurs organisationnelles qui est connue de tous, suscitant l'adhésion et l'actualisation ;
- des mesures de sensibilisation, d'information et de formation à l'éthique adaptées et accessibles à tous les paliers de l'organisation ;
- un processus d'identification des risques à l'intégrité ainsi qu'un plan d'action visant à diminuer la vulnérabilité de l'organisation face aux risques à l'intégrité (la partie 2 de ce document propose une démarche type) ;
- une ou des personnes-ressources pouvant soutenir tous les paliers de l'organisation en matière de dilemmes éthiques, de valeurs et de règles de conduite professionnelles ;
- un code de conduite contenant une déclaration officielle des valeurs organisationnelles et identifiant clairement les attentes comportementales et les conduites acceptables, à l'intention de l'ensemble du personnel et de la direction. Ce code peut aussi viser les relations avec les fournisseurs et les sous-traitants ;
- des mécanismes internes permettant :
  - d'identifier et de contrôler le lobbyisme et les communications d'influence visant les titulaires de charges publiques ;
  - de définir, de détecter, d'identifier, de mettre au jour et de sanctionner les actes répréhensibles ;
  - de signaler, en toute confiance et confidentialité, des actes répréhensibles dont un divulgateur de bonne foi est ou pourrait être témoin.

Les politiques de gestion

Les organisations élaborent des politiques de gestion et des procédures dans le but d'assurer une gouvernance et une gestion efficaces. Ces politiques doivent être robustes et contenir des mesures de détection et de lutte contre les dysfonctionnements et les écarts, peu importe leur forme. Tout comme les codes de conduite, les politiques de gestion sont des éléments importants d'une stratégie de prévention des dysfonctionnements de nature éthique ou relevant de la corruption ou d'autres actes répréhensibles. Ces politiques doivent être communiquées à tous, réalistes, claires et compréhensibles. De plus, elles doivent être revues régulièrement afin de s'assurer de leur pertinence et de leur caractère opératoire.

Les politiques de gestion des risques et de gestion de la corruption

Ces politiques de gestion informent les parties prenantes quant à la manière dont seront traités les risques organisationnels ainsi que les cas de manquements éthiques et de corruption.

Elles contiennent généralement les éléments d'information suivants :

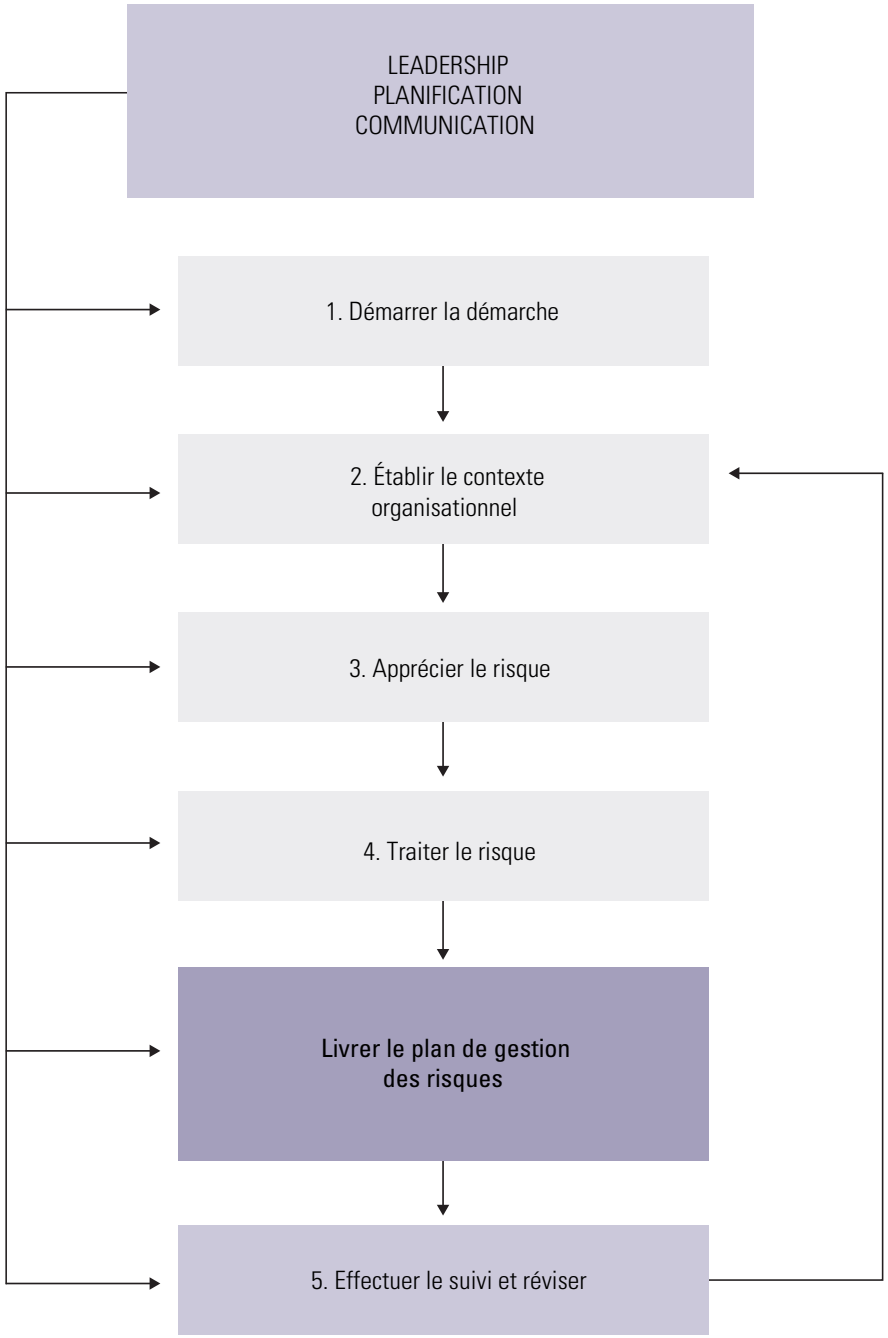
- le nom et le poste du responsable de l'application de la politique ;
- la référence aux articles des lois applicables ;
- les documents liés tels que le plan de gestion des risques à la corruption, le code de conduite, etc. ;
- la date de la dernière révision ;
- la définition des actes répréhensibles relatifs à la corruption ;
- l'énoncé des principes de gestion relatifs à la corruption ;
- le plan de communication de la politique de gestion de la corruption.

PARTIE 2

2.1 LA DÉMARCHE SUGGÉRÉE DE GESTION DES RISQUES À L'INTÉGRITÉ

L'objectif de la démarche suggérée consiste à prendre acte des risques à l'intégrité (risques éthiques et risques de corruption ou d'autres actes répréhensibles), à les analyser, les évaluer et les gérer adéquatement par un plan de gestion des risques à l'intégrité.

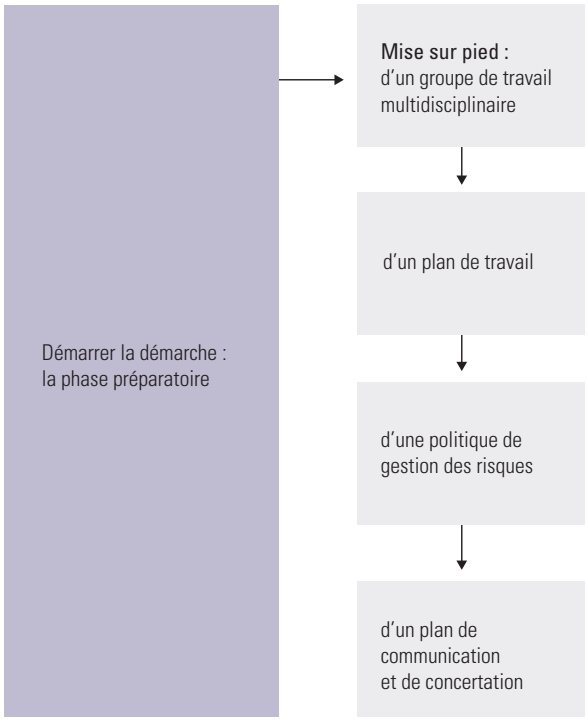
Figure 1
Étapes à suivre dans la démarche de gestion des risques à l'intégrité



2.2 DÉMARRER LA DÉMARCHE : LA PHASE PRÉPARATOIRE

La recherche de l'intégrité organisationnelle et sa consolidation passent par la participation active du plus grand nombre possible de personnes à l'examen des systèmes et des processus et au dialogue organisationnel sur les valeurs et leur actualisation.

Figure 2
Action : démarrage



2.2.1 La mise sur pied d'un groupe de travail multidisciplinaire

Les organisations sont invitées à former un groupe de travail multidisciplinaire, qui sera responsable de réaliser la démarche de gestion des risques à l'intégrité. Afin d'assurer le succès et la cohérence de la démarche, il est important de confier ce mandat à des personnes qui sont reconnues pour leurs connaissances des processus et des activités de l'organisation ainsi que pour leur leadership éthique.

Les activités d'analyse de risques à l'intégrité demandent un dialogue entre plusieurs personnes ayant des expériences diverses et pouvant communiquer et se concerter quant à leurs perceptions et leurs connaissances des différents risques à l'intégrité de l'organisation.

La composition de ce groupe doit tendre à refléter la diversité des parties prenantes à l'intérieur de l'organisation. Il sera important de susciter la participation du plus grand nombre possible de parties intéressées par les risques à l'intégrité, afin de refléter adéquatement le large éventail d'activités de l'organisation. Selon la taille de l'organisation et ses moyens, la composition du groupe de travail peut varier. L'annexe 1 présente un exemple de la composition d'un groupe de travail multidisciplinaire.

Le responsable de la gestion des risques à l'intégrité qui sera mandaté par les instances de l'organisation aux fins de la coordination du groupe multidisciplinaire devra connaître adéquatement le cheminement d'une démarche de gestion des risques. De plus, il devra faire preuve d'un grand leadership et exercer un travail rigoureux de coordination.

2.2.2 Un plan de travail

La préparation d'un plan de travail et le partage des responsabilités sont des éléments indispensables à la réalisation du plan de gestion des risques à l'intégrité dans les délais impartis. Le plan de travail consiste à déterminer toutes les activités nécessaires à la réalisation du mandat, y compris les efforts à fournir par l'ensemble des ressources impliquées.

À cette étape, il est important de déterminer quelle approche sera utilisée aux fins de l'identification des risques. Les meilleures pratiques en gestion de risques orientent ce choix vers l'approche mixte. Cette approche combine l'approche descendante et l'approche ascendante. L'approche descendante (du haut vers le bas) permet aux autorités de l'organisation d'avoir une vue globale où les risques sont au centre de l'atteinte des objectifs. L'approche ascendante (du bas vers le haut) permet l'adhésion des employés à l'exercice et renseigne l'organisation davantage sur la réalité du terrain. Une combinaison des deux approches permet à la fois d'obtenir une vue d'ensemble et d'établir une interrelation entre tous les risques identifiés de l'organisation.

Rappelons que la gestion des risques est un processus dynamique et continu, puisque les risques à l'intégrité ne sont pas statiques et que de nouveaux risques peuvent rapidement émerger. Cette démarche doit s'inscrire dans le temps, de façon rigoureuse, et être renouvelée périodiquement. Pour y arriver, il sera essentiel pour les organisations de ne pas négliger, au cours des prochaines années, la mise à jour de leurs risques à l'intégrité et d'exercer une veille stratégique sur le dossier de l'intégrité organisationnelle. Il sera important d'inscrire périodiquement une mise à jour de l'exercice, et ce, tant à l'agenda que dans les plans d'action.

Plusieurs outils informatiques de planification (suites bureautiques connues et autres applications de planification d'usage courant) permettent le fractionnement des tâches à effectuer et l'assignation des personnes nécessaires à leur réalisation, à l'intérieur de l'échéancier planifié.

2.2.3 Une politique de gestion des risques

La politique de gestion des risques constitue la déclaration des intentions et des orientations générales d'une organisation en la matière. Elle doit préciser les objectifs et les engagements de l'organisation inhérents à la gestion des risques, notamment :

- la motivation de l'organisation ;
- les liens entre les objectifs et les autres politiques de l'organisation ;
- les responsabilités ;
- la manière dont les conflits d'intérêts seront traités ;
- l'engagement de mettre les ressources nécessaires à la disposition des personnes responsables de la gestion des risques ;
- la manière dont la performance de la gestion du risque sera mesurée et communiquée ;
- l'engagement de revoir et d'améliorer périodiquement la politique et le cadre organisationnel de gestion des risques, notamment à la suite d'un événement particulier ou d'un changement de circonstances ;
- le mode de communication du contenu de la politique.

2.2.4 Un plan de communication et de concertation

Le succès de la démarche est largement tributaire de l'efficacité de la communication et de la concertation entre les différentes parties prenantes. Le processus de gestion des risques est basé sur le dialogue et la concertation de l'organisation avec les parties prenantes.

Il est recommandé d'élaborer un plan établissant les moyens à utiliser et les meilleurs moments de diffusion afin de s'assurer que l'ensemble des parties prenantes reçoit l'information nécessaire. À cet égard, l'annexe 2 donne des suggestions pour élaborer un tel plan.

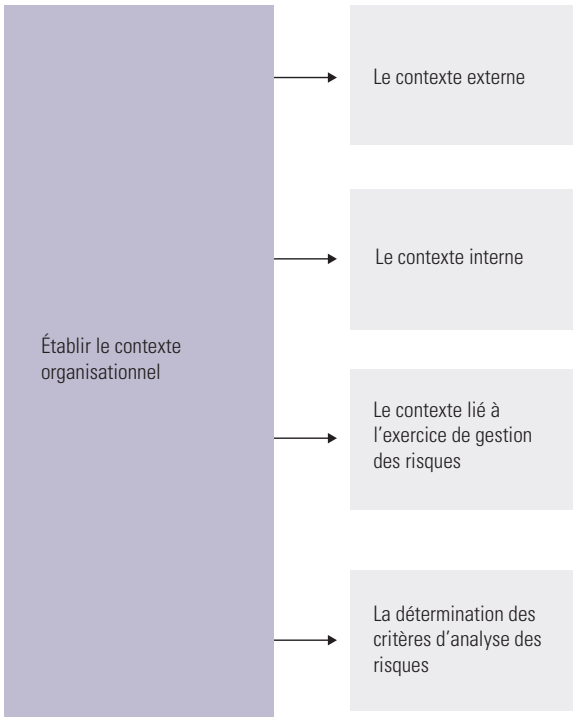
Rappelons que la concertation sera le processus de communication argumentée sur la gestion des risques avant de prendre des décisions ou déterminer une orientation. La concertation est un processus dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir. La concertation est également une contribution à la prise de décision, et non une décision conjointe.

2.3 ÉTABLIR LE CONTEXTE ORGANISATIONNEL

Les membres du groupe de travail doivent posséder une bonne connaissance du contexte organisationnel dans lequel ils évoluent.

Les derniers travaux d'identification des divers facteurs du contexte organisationnel lors de l'élaboration de la planification stratégique organisationnelle constituent le point de départ de l'analyse et de la mise à jour, le cas échéant, du contexte.

Figure 3
Action : analyse du contexte



2.3.1 Le contexte externe

L'établissement du contexte externe permettra aux membres du groupe de travail de se donner une connaissance et une compréhension communes de l'environnement dans lequel évolue l'organisation. Plus précisément, l'étude de l'environnement politique, législatif, réglementaire, économique et financier de l'organisation s'avère utile afin, notamment, d'identifier les éventuelles parties prenantes externes au processus.

En matière de qualité et d'accessibilité des services publics, il serait souhaitable d'inclure la notion d'attentes des citoyens envers les organismes donneurs de contrats publics ou fournisseurs de services. La perception des citoyens est grandement influencée par les délais de livraison, les coûts et la qualité du service ou du bien livré.

2.3.2 Le contexte interne

Une bonne compréhension du contexte interne de l'organisation influe positivement sur la qualité de la démarche. Certains éléments tels que la culture organisationnelle, la mission, la vision, les valeurs, le contexte budgétaire, le climat de travail, l'hétérogénéité des parties prenantes, les normes, les processus, les règles et la façon dont circule l'information conditionnent la précision de la démarche de gestion intégrée des risques.

2.3.3 Le contexte lié à l'exercice de gestion des risques

Les organisations qui ont déjà mis en œuvre une démarche de gestion intégrée des risques devraient inclure les risques à l'intégrité à leur démarche, et ce, afin d'obtenir un portrait complet des risques et de pouvoir considérer adéquatement les interrelations entre les divers autres risques.

Il est opportun de présenter aux membres du groupe de travail un portrait des risques déjà identifiés dans de précédents exercices de gestion des risques, le cas échéant. La personne responsable de la gestion des risques pourrait expliquer l'étendue des activités de gestion des risques à réaliser, y compris les inclusions et les exclusions particulières.

Le répondant en éthique de l'organisation peut offrir aux membres du groupe de travail une sensibilisation à l'éthique organisationnelle. Le cas échéant, il pourra les informer en leur présentant l'état de la situation du système d'éthique organisationnelle et les nouveautés en la matière (p. ex., énoncé de valeurs, nouvelles directives, grille de réflexion éthique, etc.), soit tout élément nouveau pouvant soulever des questionnements et aider au positionnement de l'organisation devant les dilemmes et les risques éthiques auxquels elle pourrait être confrontée au cours de l'exercice de gestion des risques.

2.3.4 La détermination des critères d'analyse des risques

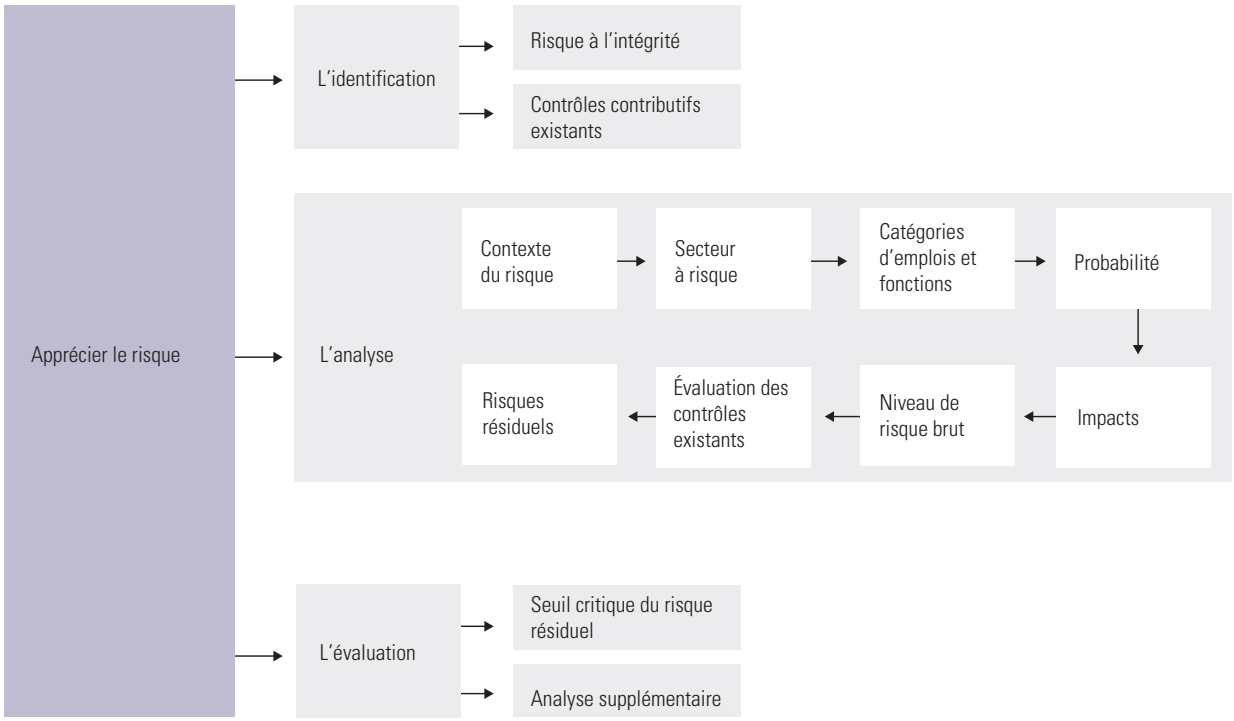
Dans le cadre de cette démarche, il appartient aux membres du groupe de travail de définir :

- la nature et les types d'**impacts** à inclure au processus de gestion des risques et la façon de les mesurer ;
- les caractéristiques des probabilités de matérialisation des risques et la façon de les mesurer ;
- la manière de déterminer le niveau d'exposition aux risques ;
- les critères permettant d'évaluer l'efficacité et l'efficience des contrôles contributifs et des mesures d'atténuation ;
- les critères permettant de décider du caractère critique d'un risque, à savoir s'il est nécessaire de traiter ce risque ou si ce risque est acceptable ou tolérable ;
- les critères permettant de mesurer la tolérance d'un risque pour l'organisation en regard de la volonté des autorités de prendre des risques.

2.4 APPRÉCIER LE RISQUE À L'INTÉGRITÉ

L'étape d'appréciation des risques à l'intégrité est constituée de l'identification, de l'analyse et de l'évaluation des risques. Elle permet d'anticiper et d'identifier les risques, d'examiner leurs causes ainsi que de prévoir leurs impacts et la probabilité de leur matérialisation. Le processus d'appréciation permettra également aux membres du groupe de travail de se pencher sur les contrôles contributifs déjà en place.

Figure 4
Action : appréciation



2.4.1 L'identification

Recherche et identification des risques à l'intégrité

Risque à l'intégrité : situation menaçant l'actualisation de la mission, des valeurs, des règles déontologiques et des dispositions légales de l'organisation pouvant causer préjudice à une ou des parties prenantes.

L'identification des risques est l'activité de recherche et de reconnaissance des risques. Elle a pour objet de déterminer les raisons pour lesquelles les objectifs de l'organisation pourraient ne pas être atteints. L'identification des risques comprend la détermination des causes des risques, par exemple les événements, les situations ou les circonstances qui seraient susceptibles d'avoir un impact sur l'atteinte des objectifs. À cet égard, l'annexe 3 donne des exemples de zones de risques à l'intégrité

Dès cette première activité, si des risques qualifiés d'intolérables apparaissaient, il reviendrait aux membres du groupe de travail de les gérer en priorité.

Il serait souhaitable de scinder la recherche des risques éthiques et celle des risques de corruption. En fait, les risques éthiques peuvent se présenter dans plusieurs processus de l'organisation, tandis que les risques de corruption sont généralement liés aux différents processus contractuels et d'offre de services. Ces deux types de risques seront par la suite réunis à l'étape de l'analyse des risques à l'intégrité.

Recherche et identification des divers risques de corruption

Risques de corruption : situations de « zones grises » où les possibilités de conduites à adopter sont multiples et où les opportunités de manquements sont les plus susceptibles de survenir. Les organisations exposées à des risques de corruption lorsqu'une ou plusieurs personnes ont la possibilité d'exercer un pouvoir décisionnel discrétionnaire ne pouvant se justifier à la lumière des règles, normes, politiques et lois applicables à l'organisation, et qui met en péril la mission de service public de l'organisation, tout en pouvant causer des préjudices aux parties prenantes.

La corruption peut s'insinuer sous de multiples formes dans plusieurs processus, s'il y a des échanges possibles ou réels entre un « corrupteur » et un « corrompu ».

Cette action consiste à examiner soigneusement les processus pour en analyser les activités et rechercher des zones de vulnérabilité pouvant ouvrir la porte à la corruption.

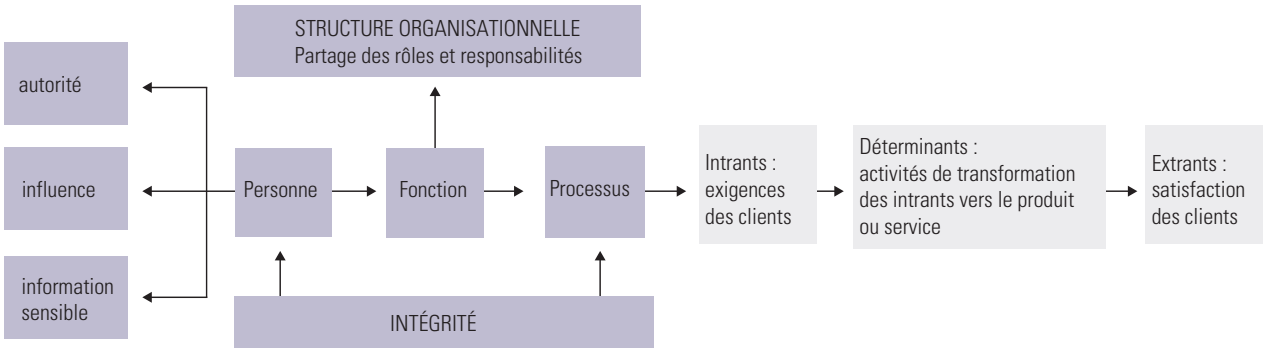
Toutes les organisations, peu importe leur envergure, gèrent à la fois des processus opérationnels constitués de leurs activités régulières et des processus plus spécifiques tels que ceux utilisés dans les processus contractuels.

Le processus d'octroi de contrats publics visant l'acquisition de biens et services constitue la zone d'étude prioritaire, compte tenu des sommes en jeu[5]. À cet égard, l'annexe 4 présente les principaux risques à l'intégrité liés à la gestion des contrats publics. Les autres processus de nature contractuelle ou apparentés à la livraison de services directs à la population et à l'octroi de subventions peuvent également constituer des zones importantes de vulnérabilité.

5 Pour consulter la Directive concernant la gestion des contrats d'approvisionnement, de services et de travaux de construction des organismes publics, consultez le lien suivant : http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/gestion_contractuelle.pdf.

Environnement des risques de corruption

Figure 5
Élément constitutif du risque à la corruption



La vulnérabilité des personnes

Toute personne subit au cours de sa vie des moments de vulnérabilité, que ce soit lors d'une rupture, d'une séparation ou du décès d'un proche, ou que ce soit dû à une frustration relative à la non-obtention d'une promotion, à un abus d'alcool, au jeu compulsif, à des problèmes financiers, etc. Pour certaines, ces moments sont de courte durée et elles retrouvent rapidement leur équilibre. Pour d'autres, par contre, leur vulnérabilité devient une opportunité pour les « corrupteurs ».

Une personne qui détient l'autorité de prendre des décisions et qui se retrouve dans un état vulnérable pourrait prendre ou omettre de prendre une décision qui favoriserait un tiers en échange d'un avantage indu. Une autre qui possède un pouvoir d'influence auprès d'un décideur pourrait utiliser cette influence dans le but de favoriser un « corrupteur » en échange d'un avantage.

Finalement, une personne qui détient de l'information sensible pourrait être tentée, si elle est vulnérable, de donner cette information à un « corrupteur » en échange d'un avantage.

Dans la plupart des cas, ce n'est pas la personne qui demande ou offre à un « corrupteur » de faire ou d'omettre de faire quelque chose qui pourrait l'avantager. Ce sont plutôt les « corrupteurs » qui, informés de la vulnérabilité d'une personne, tenteront de la convaincre de collaborer avec eux. Quelques fois, les « corrupteurs » iront même jusqu'à utiliser la menace dans le but de forcer des personnes à leur donner ce qu'ils veulent.

Pour identifier les risques à l'intégrité relatifs aux personnes, il serait pertinent de se poser les questions suivantes : « Quelles sont les parties prenantes qui sont directement ou indirectement impliquées dans les processus contractuels? Quelles sont les personnes qui possèdent le pouvoir d'autoriser les dépenses et les achats? Quelles sont les personnes qui ont une influence sur les décisions? Quelles sont les personnes qui détiennent de l'information sensible? ».

La vulnérabilité des fonctions

Toutes les organisations développent des structures organisationnelles dans le but de réaliser efficacement leur mission et leurs mandats. La répartition des rôles et des responsabilités est l'un des éléments importants de cette structuration.

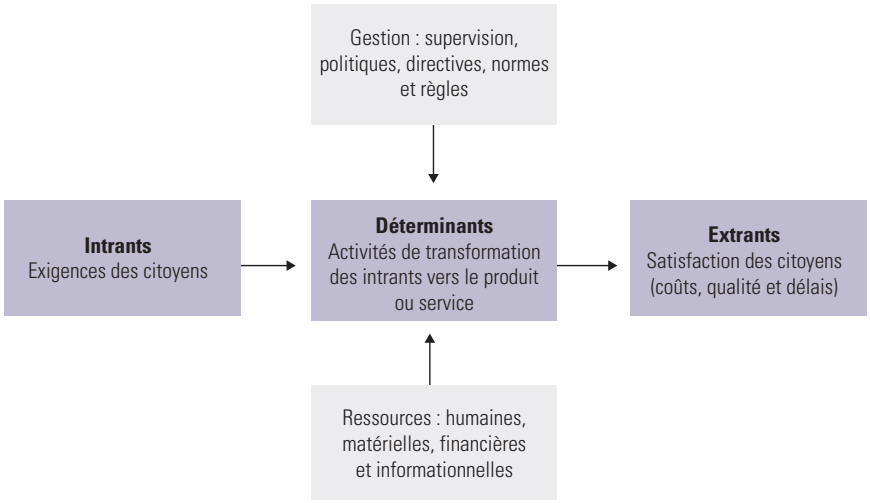
Cependant, très peu d'organisations se demandent si la concentration des pouvoirs et des responsabilités dans les fonctions inhérentes à certains postes ne favorise pas l'émergence de vulnérabilités et ne constitue pas une occasion pour les « corrupteurs ». En effet, il arrive que la concentration de responsabilités dans certaines fonctions fasse en sorte que c'est la même personne qui identifie les besoins, rédige les appels d'offres et signe les contrats.

Une analyse de la sensibilité des fonctions et des emplois est une méthode utile afin de déterminer le niveau de vulnérabilité et d'établir quels moyens pourraient être mis en place pour en atténuer les risques. À cet égard, l'annexe 5 présente les principaux risques associés à l'emploi ou à la personne.

La vulnérabilité des processus

Un processus est défini comme l'ensemble des activités qui transforment des intrants en extrants. Quant aux procédures, ce sont des manières ou façons précises d'accomplir une activité. Il s'agit généralement d'instructions et de règles explicites et codifiées.

Figure 6
Élément constituants d'un processus



Les types de processus

Les processus de direction sont les règles de fonctionnement des opérations régulières de l'organisation, régissant la manière dont les activités du processus déterminant fonctionnent. Ce sont, notamment, les normes de production, les règles de fonctionnement interne et le mode de supervision utilisés dans l'organisation.

Les processus déterminants contribuent au respect des exigences qualitatives et quantitatives et déterminent le produit ou le service, soit les extrants.

Les processus de soutien contribuent au bon déroulement du processus déterminant, en fournissant les ressources nécessaires au bon moment.

Ces trois types de processus se distinguent par la nature de leurs extrants, comme le décrit le tableau 1, présenté ci-après.

Tableau 1
Types de processus

Typologie	Extrants
Processus de direction	Décisions
Processus déterminants	Produits ou services
Processus de soutien	Ressources

On peut donc rapidement identifier les risques qui pourraient apparaître en fonction du type de processus. Les processus de direction peuvent contenir des vulnérabilités si des décisions favorisant un tiers en échange d'un avantage étaient prises. Quant aux processus déterminants, ils pourraient contenir des vulnérabilités en fonction de la description des

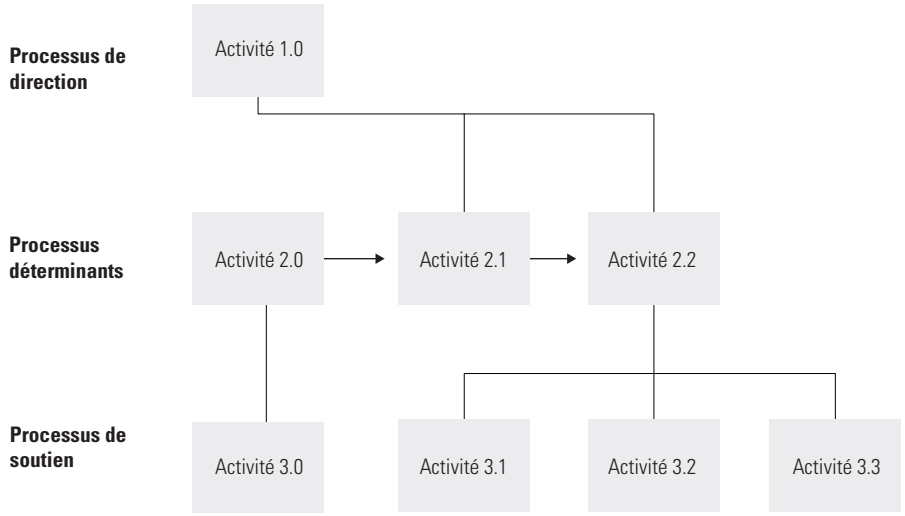
produits ou des services qui favoriseraient un fournisseur au détriment des autres ou encore en échange d'un avantage. Finalement, les processus de soutien pourraient contenir des vulnérabilités si les ressources financières (surévaluation, extras, etc.), matérielles (qualité ou quantité des produits) ou humaines (expertises, nombre, etc.) sont modifiées dans le but de favoriser un tiers en échange d'un avantage.

La description des activités

À partir de l'identification des processus, réalisée par les différentes directions de l'organisation, il faut procéder à une analyse plus méthodique en dressant la liste des activités constituantes de chacun de ces processus.

L'approche préconisée consiste à réaliser un diagramme de l'ensemble des processus, en y indiquant les liens qui existent entre eux. Il faut tenter d'identifier les activités constituantes du processus en déclinant les activités des processus de direction, celles des processus déterminants et, enfin, celles des processus de soutien.

Figure 7
Type de processus et activités



La compréhension des activités constituantes des phases de gestion des services publics est essentielle si l'on veut être en mesure d'identifier les failles potentielles ouvrant la porte à la corruption.

Comme nous l'avons énoncé précédemment, le processus de gestion des contrats publics d'acquisition de biens et services constitue la porte d'entrée privilégiée de la corruption dans une organisation.

Recherche et identification des risques éthiques

Risques éthiques : situations de « zones grises » où les possibilités de conduites à adopter sont multiples et où les opportunités de manquements sont les plus susceptibles de survenir. Les organisations sont exposées à des risques en matière d'éthique lorsqu'une ou plusieurs personnes ont la possibilité d'adopter des comportements qui ne peuvent se justifier à la lumière des valeurs partagées au sein de l'organisation, ou qui mettent en péril la mission de l'organisation, tout en pouvant causer des préjudices aux parties prenantes.

Les risques de nature éthique que nous qualifierons de systémiques peuvent se retrouver dans le système d'éthique de l'organisation. Il appartient d'abord aux membres du groupe de travail d'examiner :

- les valeurs organisationnelles, leur appropriation et leur actualisation par l'ensemble du personnel ;
- les outils déontologiques, leur pertinence, leur clarté et leur application ;

- les mesures de sensibilisation et de formation à l'éthique et à la déontologie ;
- les services-conseils en matière d'éthique ;
- les activités de reconnaissance et les moyens utilisés à cette fin, visant à souligner les comportements éthiques du personnel contribuant au renforcement de la culture organisationnelle d'intégrité ;
- les activités de sensibilisation et de formation ainsi que les contrôles des activités de lobbyisme ou de communication d'influence dont l'organisation peut faire l'objet ;
- les modes de fonctionnement relatifs à la divulgation d'actes répréhensibles ;
- les capacités organisationnelles d'identification, d'examen et d'analyse ainsi que les mesures de contrôle et de sanction mises en place relativement aux actes répréhensibles.

Par la suite, le travail du comité consistera à rechercher chacun des risques éthiques dans chacun des processus de l'organisation, et non pas uniquement dans les processus où sont déjà identifiés des risques de corruption ou d'autres actes répréhensibles. L'annexe 3 présente des exemples de zones de risques à l'intégrité.

L'enjeu principal de l'identification des risques de nature éthique ne peut s'arrêter au seul examen des règles applicables dans l'organisation. Cette action nécessite de distinguer le risque éthique du dilemme de nature éthique. Le dilemme éthique se matérialise lorsque des valeurs organisationnelles se confrontent dans certains processus. Quant au risque de nature éthique, il se retrouvera dans des comportements non justifiables au regard des valeurs et de la mission de l'organisation.

Exemples

- Le dilemme émanant de la confrontation des valeurs de loyauté et de discrétion lors de la divulgation de la commission d'actes répréhensibles.
- Le risque se matérialisant dans la proximité entre un titulaire de charge publique et un quelconque lobby, sans un encadrement approprié.

Les risques éthiques ne constituent pas tous des dilemmes de nature éthique et les dilemmes éthiques ne constituent pas tous des risques. Les dilemmes sont inévitables ; il est toutefois indispensable que l'organisation soit informée de leur existence. Il peut être pertinent de laisser subsister ces dilemmes, tout en soutenant le personnel exposé dans le cadre de leur gestion. Une culture organisationnelle d'intégrité reposera sur l'équilibre entre l'actualisation des valeurs et la gestion par les règles.

Bien que les risques de nature éthique puissent se retrouver dans plusieurs processus de l'organisation, les zones de risques éthiques à étudier en priorité sont les suivantes :

- la gestion des ressources humaines ;
- l'acquisition de biens et services ;
- les processus de services aux diverses clientèles et parties prenantes de l'organisation ;
- la gouvernance.

L'objectif est de faire un premier balayage afin d'obtenir le portrait général des risques éthiques de l'organisation, même si ces derniers ont déjà été gérés.

Dans le même ordre d'idées, les éléments suivants constituent des sources permettant d'identifier des zones de risques éthiques :

- l'analyse de la récurrence de certaines thématiques lors des demandes de consultation ou de conseil en matière d'éthique ou de déontologie auprès des répondants en éthique, des gestionnaires ou des autorités de l'organisation ;
- le recensement des thématiques des avis éthiques rédigés par le répondant en éthique au fil des ans ;
- les précédentes analyses organisationnelles de dilemmes éthiques ;
- les plaintes reçues par l'organisation et portant sur la qualité des services de l'organisation, leur accessibilité ou le comportement du personnel ;
- les problématiques étudiées par le comité d'éthique organisationnelle.

Identification des contrôles contributifs existants

À chacun des risques identifiés lors des actions précédentes, il y aura lieu d'associer les contrôles contributifs existants. C'est à ce moment qu'il faut recenser l'ensemble des moyens déjà mis en place pouvant être utiles au contrôle du risque identifié précédemment. C'est également dans le cadre de cette action que les membres du groupe de travail pourraient constater l'absence de moyens contribuant à l'atténuation du risque.

2.4.2 L'analyse

Les actions suivantes permettent de replacer chacun des risques dans son contexte, de déterminer ses impacts et ses probabilités de matérialisation. L'importance accordée à l'analyse de tous les éléments du contexte de chacun des risques permettra de mieux saisir les conséquences des préjudices potentiels à l'endroit de l'organisation ou de diverses parties prenantes. L'annexe 6 suggère un tableau permettant le regroupement des risques identifiés.

Contexte de chacun des risques à l'intégrité

Il importe de bien documenter les sources et le contexte d'émergence du risque, c'est-à-dire le ou les facteurs internes ou externes qui alimentent ou donnent naissance à un risque.

Exemples

- Est-ce que le risque émerge toujours à la même période de l'année?
- Est-ce que le risque survient dans le cadre d'activités ou de processus stratégiques?
- Est-ce que le risque touche les relations avec les clientèles externes?
- Quelles sont les parties prenantes du risque?
- Est-ce que les budgets alloués alimentent le risque?
- Etc.

Identification des secteurs à risque

Cette activité ciblera, pour chacun des risques à l'intégrité, quel secteur de l'organisation est touché.

Exemples

- La gestion des ressources humaines
- L'acquisition de biens et services
- L'octroi de subventions
- Etc.

Chaque organisation pouvant avoir des structures différentes, ces secteurs peuvent varier. Le regroupement de certains risques permettra ainsi de cibler des secteurs particuliers où l'on peut retrouver une concentration plus élevée de risques. La récurrence d'un même risque dans plusieurs secteurs d'activités de l'organisation peut aussi démontrer la nécessité de traiter ce même risque en collaboration avec l'ensemble des unités exposées.

Identification des catégories d'emplois et des fonctions potentiellement à risque

Il s'agit ici d'identifier les catégories d'emplois et les fonctions exposées à un risque donné. Quelles sont les catégories d'employés ou parties prenantes de l'organisation qui sont au cœur du risque à l'intégrité?

Exemples

- Est-ce qu'une équipe de techniciens assignée au fonctionnement d'un processus d'émission de permis est particulièrement exposée au risque?
- Les professionnels chargés d'analyser des demandes provenant du public sont-ils plus exposés à un risque donné que les professionnels de l'équipe de la direction chargée de concevoir les politiques de l'organisation?
- Ces catégories de personnel représentent-elles un pourcentage élevé des employés de l'organisation?
- Ces employés travaillent-ils de près ou de loin avec des firmes externes?
- Sont-ils étudiants, stagiaires, occasionnels ou permanents?
- Sont-ils techniciens, professionnels, gestionnaires?
- Quelle est leur fréquence d'exposition au risque?

Dans le cadre de cette action, il est recommandé de ne pas approfondir au point d'identifier une personne en particulier.

Ce questionnement permettra de mieux cibler les interventions nécessaires (information générale, sensibilisation, formation, intervention ciblée par équipe) pour réduire les risques, sans nécessiter des interventions auprès de l'ensemble des employés, mais plutôt uniquement auprès de ceux qui sont les plus exposés à des risques.

Mesure de la probabilité du risque à l'intégrité

Pour la mesure de la probabilité, il s'agit de se demander quelle est la probabilité que le risque à l'intégrité se matérialise, et ce, sans considérer l'efficacité des contrôles contributifs existants.

Exemples

- Le risque s'est-il déjà matérialisé par le passé?
- Est-ce qu'un événement récent laisse croire que ce risque s'est déjà matérialisé ou pourrait se reproduire?
- Si aucune mesure n'était prise, quelle serait la probabilité que le risque se matérialise?

L'utilisation de données historiques pertinentes peut s'avérer utile à cette étape. Les éléments constituants du contexte de chacun des risques identifiés permettent aussi de préciser cette mesure de la probabilité de matérialisation.

Mesure des impacts du risque à l'intégrité

Cette action vise à mesurer l'impact prévisible du risque identifié, et ce, sans considérer l'efficacité des contrôles contributifs existants. Il s'agit de se demander quel serait l'impact réel de ce risque sur l'organisation s'il se matérialisait.

Exemples - en cas de matérialisation

- Quelles seraient les conséquences pour l'image de l'organisation?
- Qui serait touché (citoyens, partenaires, employés, élus, population et autres parties prenantes)?
- Quelle serait l'importance des éventuels préjudices subis?
- Quelles seraient les réactions des parties prenantes?
- Quelles seraient les répercussions globales sur l'organisation?

Le tableau 2, présenté ci-après, suggère une échelle des mesures des probabilités et des impacts.

Tableau 2
Échelle suggérée des mesures des probabilités et des impacts

Cote
1 (Très faible)
2 (Faible)
3 (Modérée)
4 (Élevée)
5 (Très élevée)

Niveau de risque brut

Le tableau 3, présenté ci-après, donne des exemples de niveaux d'exposition au risque brut à l'intégrité. Le niveau de risque brut à l'intégrité est obtenu par la multiplication de la cote attribué à la probabilité par celle attribuée à l'impact.

Tableau 3
Exemples de niveaux d'exposition au risque brut à l'intégrité

NIVEAU D'EXPOSITION AU RISQUE = impact x probabilité

		Probabilité				
		Très faible (1)	Faible (2)	Modérée (3)	Élevée (4)	Très élevée (5)
Impact	Très élevé (5)	5	10	15	20	25
	Élevé (4)	4	8	12	16	20
	Modéré (3)	3	6	9	12	15
	Faible (2)	2	4	6	8	10
	Très faible (1)	1	2	3	4	5

Évaluation des contrôles contributifs existants

La démarche consistera ensuite à se demander si des contrôles contributifs sont en place pour atténuer les risques identifiés, à savoir si l'organisation gère actuellement le risque à l'intégrité de façon concrète. Il est possible qu'aucun mécanisme ne soit en place. Ce constat permettra d'alimenter les prochaines étapes du processus.

Pour chacun des risques, il faut évaluer les contrôles contributifs existants liés à ce risque particulier et se poser les questions suivantes :

- Ces contrôles sont-ils adéquats pour traiter le risque et le maintenir à un niveau modéré?
- Les contrôles déjà en place fonctionnent-ils efficacement?
- Cette efficacité peut-elle être démontrée au besoin?

L'annexe 7 suggère un tableau permettant de regrouper les risques restant à évalués.

Le tableau 4, présenté ci-après, donne des exemples de coefficients d'atténuation du niveau de risque à attribuer à chacun des risques à l'intégrité, selon l'efficacité des contrôles contributifs identifiés.

Tableau 4
Exemple d'échelle des coefficients d'atténuation du risque brut à l'intégrité par les contrôles contributifs existants

Cote	Contrôles contributifs	Description	Coefficients d'atténuation
1	Inexistant	Aucun contrôle contributif	0 %
2	Insuffisant	Contrôles contributifs/mesures d'atténuation/insuffisants (actions importantes requises pour réduire le risque au-dessous du seuil de tolérance)	25 %
3	Quasi satisfaisant	Risque couvert partiellement (actions peu significatives pour réduire le risque au-dessous du seuil de tolérance)	50 %
4	Satisfaisant	Risque couvert efficacement (risque réduit au-dessous du seuil de tolérance)	75 %

Mesure du risque résiduel à l'intégrité

Dans le cadre de cette activité, le groupe de travail doit déterminer le niveau de risque résiduel à l'intégrité. Le risque résiduel désigne le risque auquel l'organisation demeure exposée en tenant compte de l'efficacité des contrôles contributifs déjà en place pour réduire le niveau de risque. Concrètement, il s'agit de réduire le niveau de risque brut par l'application du coefficient d'atténuation.

NIVEAU DE RISQUE RÉSIDUEL =
niveau de risque brut – (niveau de risque brut x coefficients d'atténuation)

2.4.3 L'évaluation

Seuil critique du risque résiduel à l'intégrité

Les risques résiduels à l'intégrité sont maintenant identifiés, caractérisés et mis en contexte, et l'efficacité des contrôles contributifs inhérents est mesurée.

Les membres du groupe de travail doivent ensuite se demander quel est le seuil de tolérance acceptable pour l'organisation devant le risque net à l'intégrité. Il s'agit d'expliquer pourquoi l'organisation a décidé d'accepter ou de rejeter un niveau donné de risque résiduel. Il est à noter que la tolérance à un même risque pourrait varier au sein de deux organisations différentes.

Cette étape permettra aux membres du groupe de travail :

- d'identifier les risques non significatifs ne nécessitant pas de traitement ;
  - idéalement, ces risques seront surveillés et revus lors de la mise à jour cyclique du plan de gestion des risques.
- de poursuivre une évaluation et une analyse plus détaillées du risque ;
  - ce type de risque nécessite une étude attentive avant d'être traité.
- de traiter le risque sans évaluation supplémentaire ;
  - le seuil critique du risque étant évident, le risque doit être traité lors de la prochaine étape.

Il faut que la tolérance au risque soit claire, comprise et partagée à tous les niveaux de l'organisation, afin de permettre une prise de décision éclairée. Le tableau 5, présenté ci-après, donne des exemples de niveaux d'exposition au risque résiduel à l'intégrité.

Tableau 5
Exemples de niveaux d'exposition au risque résiduel à l'intégrité

Niveau d'exposition	Description
1-2 Très faible	Le risque résiduel à l'intégrité est très faible et facilement acceptable. Les contrôles contributifs actuels sont suffisants et aucune mesure supplémentaire n'est nécessaire.
3-4 Faible	Le risque résiduel à l'intégrité est faible et acceptable. Toutefois, ce risque pourrait nécessiter un suivi, si ce dernier n'exige pas trop de temps, de coûts ou de ressources substantielles. Les contrôles contributifs actuels sont suffisants, mais il faut s'assurer qu'ils demeurent en place. Aucune mesure supplémentaire n'est requise.
5-9 Modéré	Le risque résiduel à l'intégrité est modéré, mais doit tout de même être géré adéquatement à court ou à moyen terme. Il faut envisager de diminuer le risque, s'il y a lieu, à un niveau faible, tout en tenant compte des coûts de mise en place de certaines mesures.
10-15 Élevé	Le risque résiduel à l'intégrité est élevé. Des mesures importantes visant à réduire le risque doivent rapidement être mises en œuvre dans un délai clairement défini. Il peut être nécessaire d'envisager d'interrompre ou de restreindre l'activité ou de mettre en place des mesures de contrôle contributif intérimaires visant la réduction de ce risque jusqu'à ce que des mesures permanentes soient adoptées. Il peut également être nécessaire d'investir des ressources considérables pour mettre en place des mesures de maîtrise additionnelles. Il est essentiel de gérer ce risque et d'en faire un suivi dans les plus brefs délais.
16-25 Très élevé	Le risque résiduel à l'intégrité est très élevé et doit rapidement faire l'objet d'une gestion serrée. Des améliorations importantes concernant les mesures de maîtrise de ce risque sont nécessaires pour le réduire à un niveau faible ou modéré. En attendant la mise en place éventuelle de ces mesures, il faut envisager de mettre fin aux activités qui conduisent à ce risque.

Analyse supplémentaire de certains risques

Une analyse supplémentaire s'avérera nécessaire pour certains risques. Lorsqu'un risque se situe dans une « zone grise » ou qu'il présente un seuil critique flou, des impacts incertains ou des chevauchements avec d'autres risques, les membres du groupe de travail devraient se pencher sur une évaluation supplémentaire.

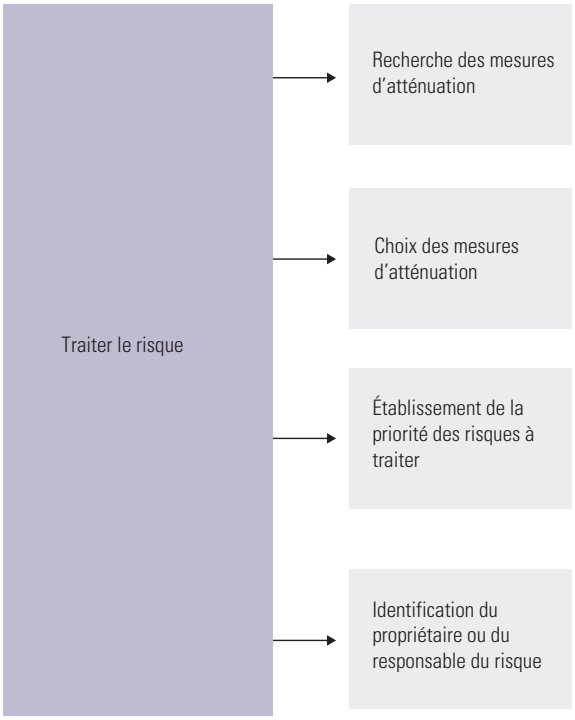
Cette étape exige de définir plus précisément ces risques éthiques ou de corruption ainsi que de réexaminer leur contexte, de même que les processus et les activités où ils ont été repérés, à la lumière des critères préalablement définis. Ils seront aussi réétudiés par rapport aux impacts financiers et légaux et à la perception des parties prenantes.

Notons ici qu'il est important de faire une description détaillée de ces risques. Si les étapes précédentes ont été réalisées adéquatement, cette étape devrait être plus précise et plus nuancée que celle de la recherche et de l'identification des risques.

2.5 TRAITER LE RISQUE

Maintenant que les actions nécessaires à l'appréciation des risques sont réalisées, le traitement des risques implique de choisir et d'accepter une ou plusieurs options permettant de réduire la probabilité de matérialisation et d'atténuer les impacts de chacun des risques résiduels présentant un niveau d'exposition jugé modéré, élevé ou très élevé.

Figure 8
Action : traitement du risque



2.5.1 Recherche des mesures d'atténuation

Cette action consiste à produire des mesures d'atténuation qui permettront d'accepter le risque, de l'annuler, de le réduire à un niveau acceptable ou de le transférer à une autre entité.

Outre les membres du groupe de travail multidisciplinaire, le responsable pourra s'adjoindre les personnes qui ont les meilleures connaissances des processus, par exemple les experts en octroi de contrats publics ou en éthique, afin de suggérer les mesures potentielles d'atténuation de chacun des risques précédemment identifiés.

Il existe plusieurs façons de réaliser cet exercice. Il est recommandé de procéder par la méthode du remue-méninges, laquelle donne d'excellents résultats dans un délai relativement court[6] .

Plus particulièrement, pour atténuer les risques liés à certaines personnes ou fonctions en matière de corruption ou relativement à d'autres actes répréhensibles, les moyens les plus efficaces sont le double regard et les contrôles (planifiés et d'exception). À cet égard, l'annexe 5 présente les risques associés à l'emploi ou à la personne.

6 Les liens suivants peuvent guider le choix d'outils utiles :
http://guidesaideconception.uqar.ca/wp-content/uploads/2015/02/Fiche_Remue_méninges.pdf;
http://www.iaat.org/telechargement/guide_methodo/stimuler_idees.pdf;
http://oqi.wisc.edu/resourcelibrary/uploads/resources/Facilitator%20Tool%20Kit.pdf.

2.5.2 Choix des mesures d'atténuation

Parmi les mesures d'atténuation précédemment identifiées, il convient de retenir celles qui permettront de produire les effets escomptés sur le risque résiduel identifié. Soulignons que la robustesse des mesures identifiées à cette étape doit être proportionnelle au seuil critique du risque à réduire ou à éliminer. Il convient donc de se poser les questions suivantes :

- La mesure d'atténuation réduit-elle significativement les impacts ou les possibilités de matérialisation du risque, ou les deux, préalablement identifiés pour ce même risque?
- Les mesures proposées peuvent-elles être mises en place facilement, à un coût raisonnable?
- Quels sont les impacts de la nouvelle mesure choisie sur les parties prenantes?
- Le contrôle contributif déjà en place doit-il être mis à jour, amendé ou complètement revu?
- Devant la lourdeur des nouvelles mesures d'atténuation à mettre en place, vaut-il mieux accepter le risque?
  - Dans ce dernier cas, la possibilité d'exposition au risque augmente-t-elle?
- Comment sera mesurée l'efficience de la mesure d'atténuation?
- Par quels moyens vérifiera-t-on l'efficience de la mesure d'atténuation choisie?
- La mise en place de la mesure d'atténuation choisie fera-t-elle émerger un nouveau risque d'un autre type?
  - Si oui, le nouveau risque sera-t-il moindre ou pire que le risque original?

Le choix d'une mesure d'atténuation donnée, parmi celles identifiées, peut donner naissance à un conflit de valeurs ou de règles. Le dilemme d'actions ainsi créé devrait être analysé. L'outil à privilégier à cette fin par le répondant en éthique est la Grille d'aide à la décision éthique, présentée à l'annexe 8, extraite de la Trousse de référence à l'intention des répondantes et répondants en éthique de la fonction publique du Québec ou le Guide pour la rédaction d'un avis éthique, présenté à l'annexe 9. Cette approche constitue un complément aux techniques reconnues en matière de gestion de risques.

Exemple de mesures d'atténuation

- L'écoute et l'enregistrement des demandes de renseignements téléphoniques créent-ils une atteinte à l'expectative normale de vie privée du personnel ou des demandeurs de renseignements? (dilemme entre efficacité et confidentialité)
- Les vérifications supplémentaires a priori rallongeant les délais de traitement d'une demande de subvention aux entreprises créent-elles de possibles préjudices aux demandeurs? (dilemme entre célérité du service et rigueur administrative)

2.5.3 Établissement de la priorité des risques à traiter

Cette étape consiste à établir des priorités quant aux risques à traiter en fonction des seuils critiques identifiés précédemment. Cette étape permettra ainsi à l'organisation de mettre en œuvre un plan de gestion des risques, de surveiller, d'évaluer et de réviser la performance des moyens utilisés pour les atténuer et, enfin, de communiquer les résultats de l'exercice d'identification des risques à l'intégrité.

Le plan de gestion des risques est un document dynamique présentant les mesures d'atténuation qui seront mises en place. À cet égard, l'annexe 10 présente un gabarit pouvant être utilisé pour rédiger le plan de gestion des risques et l'annexe 11 en présente un modèle. De plus, le plan identifiera le responsable de la mise en place de la mesure d'atténuation, le moment de sa mise en place et la manière utilisée pour ce faire et, surtout, le moyen qui sera utilisé pour évaluer la performance de cette mesure par un indicateur.

Il importe de souligner que les risques et les mesures d'atténuation retenus pour l'élaboration du plan de gestion des risques pouvant toucher la gestion de certains projets en cours d'élaboration ou de réalisation (contrats d'acquisition de biens ou de services, de construction, etc.) devront être intégrés aux plans de ces mêmes projets. Ces risques et les mesures d'atténuation afférentes seront alors suivis en fonction des échéanciers prévus aux plans de projets, afin d'en déterminer la pertinence et l'efficacité.

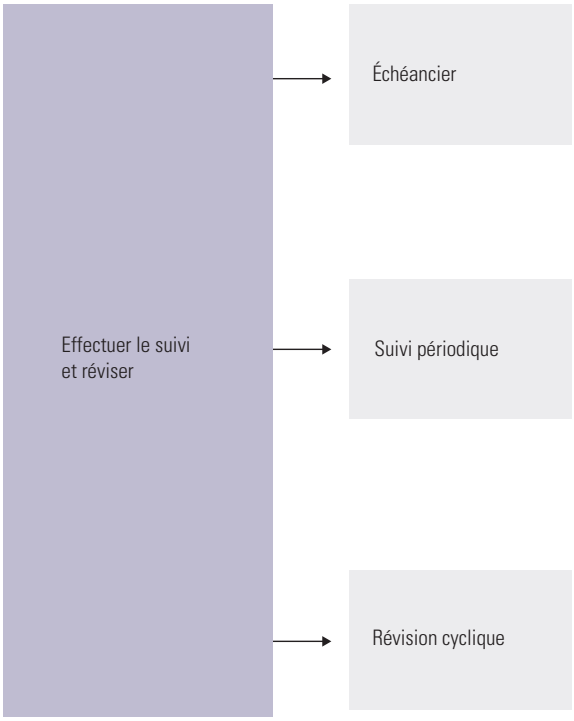
Dans le cas où de nouveaux risques se présentent, il faut les traiter dès leur apparition et les inclure au plan, en fonction de leur priorité. Les coûts d'implantation et de suivi des mesures d'atténuation du risque d'un contrat doivent être imputés, le cas échéant, au contrat lui-même et suivis par le responsable au même titre que les autres indicateurs de réalisation.

2.5.4 Identification du propriétaire ou responsable du risque

Cette étape vise à identifier un responsable de la gestion du risque à l'intégrité, à savoir le nom de la personne de l'organisation qui aura le mandat de faire le suivi de ce risque, de le réduire ou de l'éliminer, et le nom de la personne qui sera responsable d'implanter des mesures d'atténuation. Généralement, la gestion d'un risque est confiée à son propriétaire, qui pourra s'adjoindre des collaborateurs, au besoin.

2.6 EFFECTUER LE SUIVI ET RÉVISER

Figure 9
Action : suivi et révision du plan de gestion des risques



2.6.1 Échéancier

L'établissement d'un échéancier est nécessaire pour la mise en place des mesures visant à atténuer chacun des risques.

2.6.2 Suivi périodique

La maîtrise du plan de gestion des risques à l'intégrité exige également un contrôle rigoureux de l'implantation des mesures d'atténuation sélectionnées. Il faut en assurer le suivi et la correction rapide dans le cas où ces mesures ne donneraient pas les résultats escomptés.

2.6.3 Révision cyclique

La maîtrise du plan de gestion des risques à l'intégrité passe nécessairement par la mise à jour régulière des risques et des mesures d'atténuation, selon les règles de contrôle et de vérification applicables dans l'organisation. Cette révision cyclique n'exclut pas la nécessité de revoir le plan d'action lors de l'apparition d'un nouveau risque ayant des impacts immédiats. Les membres du groupe de travail peuvent amorcer les travaux de suivi et de révision en se posant les questions suivantes :

- Les hypothèses ou les constats formulés à l'étape de la recherche et de l'identification des risques sont-ils toujours d'actualité?
- Les contextes interne et externe ont-ils été modifiés significativement?
- Les mesures d'atténuation mises en place ont-elles été efficaces?
- Les résultats escomptés dans le plan ont-ils été atteints?

CONCLUSION

L'expertise de l'UPAC et du SCT, l'apport d'experts d'organisations publiques et la documentation disponible nous auront permis de proposer la stratégie et la démarche décrites dans le présent document, issues des meilleures pratiques. Nous n'avons toutefois pas la prétention de proposer une démarche clés en main, mais plutôt de permettre aux organisations publiques de se mettre en action pour identifier et prévenir de manière proactive les risques à l'intégrité.

La démarche proposée ne requiert pas l'implantation d'un nouveau système de gestion. La plupart du temps, elle fait appel à de l'information déjà disponible dans l'organisation.

Puisqu'il est reconnu que les problèmes liés à l'intégrité peuvent prendre source à tous les niveaux de l'organisation, la démarche devra donc s'appuyer sur des échanges de bas en haut, de haut en bas, et transversaux, au sein de cette même organisation. De plus, puisque la démarche est construite autour des connaissances des processus par les membres de l'organisation, elle permet de valoriser ceux-ci et de les intéresser à l'actualisation de leurs compétences éthiques.

La démarche de gestion des risques à l'intégrité constitue un outil d'aide à la décision stratégique pour une haute direction soucieuse de maintenir et de consolider sa culture d'intégrité. En bout de piste, elle offre à l'organisation la possibilité d'une gestion préventive de son intégrité organisationnelle adaptée à sa réalité. En ce sens, l'organisation aura un traitement adapté et modulé de ses risques, tant éthiques que de corruption. À ce stade, de nombreuses approches sont possibles, que ce soit d'éliminer ou de rejeter le risque, de réduire le risque à un niveau acceptable, de transférer le risque, ou de l'accepter tel qu'il est, mais en le justifiant et en le surveillant.

L'objectif étant de favoriser l'adhésion et la participation de l'ensemble du personnel, il serait opportun qu'une stratégie de communication interne et de gestion du changement soit incluse dans le plan de mise en œuvre.

L'UPAC et le SCT, par l'entremise de leurs équipes de spécialistes, veulent encourager et faciliter l'implantation de plans de prévention et de gestion des risques au sein des organisations publiques. Pour ce faire, elles offrent un rôle-conseil quant aux meilleures pratiques et un accompagnement pour les organisations.

ANNEXE 1

Exemple de la composition d'un groupe de travail multidisciplinaire

- **Un représentant de la haute direction**
  - (sous-ministre, sous-ministre adjoint ou associé, président, vice-président, directeur général)
- **Une personne spécialisée dans la gestion des risques**
- **Le répondant en éthique de l'organisation**
- **Un membre provenant de chaque direction de l'organisation, en particulier :**
  - une personne de la Direction des communications ;
  - une personne de la Direction des ressources humaines ;
  - une personne de la Direction des affaires juridiques ;
  - une personne du Secrétariat général ;
  - une personne de la Direction de l'administration ;
  - une ou des personnes des directions opérationnelles ;
  - une personne des services de la sécurité de l'information ;
  - une personne de la Direction de la vérification ou de l'audit interne ;
  - le responsable de l'observation des règles contractuelles, etc.

ANNEXE 2

Contenu suggéré d'un plan de communication

Contexte de la communication	Brève description de l'historique du projet et des dates charnières, ainsi que des décisions et des éléments significatifs qui ont conduit à l'élaboration et à la mise en œuvre du plan de communication. Cette description sert à expliquer la raison de la mise en place de ce processus.
Enjeux	Quels sont les éléments pouvant avoir des répercussions sur les personnes ou les processus de l'organisation qui devront être pris en compte dans la mise en place du processus de gestion des risques à l'intégrité? Cette partie vise donc à identifier les résistances ou oppositions qui pourraient se matérialiser en cours de route, mais également les éléments qui seront favorables au projet.
Objectifs	Quel est l'objectif visé exactement par le plan de communication? Quelle est la situation souhaitée (accroître, informer, rassurer, etc.)? Les objectifs répondent généralement aux questions « Qui? Quoi? Quand? Où? ». Un objectif doit être suffisamment précis pour qu'il puisse être évalué et, si possible, quantifié. Un objectif principal peut avoir plusieurs objectifs secondaires. Exemple : Objectif principal : Informer les employés de la mise en place d'une approche de gestion des risques à l'intégrité dans l'organisation. Objectif secondaire 1 : Rassurer les employés sur leur lien d'emploi. Objectif secondaire 2 : Favoriser leur adhésion et leur collaboration.
Clientèle cible	Il est important de bien déterminer à qui ce plan de communication s'adresse exactement. La mise en place d'un processus de gestion des risques à l'intégrité touchera, de plus ou moins près, un grand nombre de personnes dans l'organisation. Il aura aussi des répercussions sur d'autres personnes et organisations externes telles que des fournisseurs ou des partenaires. Pour accroître l'appui au projet, il faut donc penser à toutes les parties prenantes qui seront concernées de près ou de loin et déterminer l'information dont chacune aura besoin.
Axe de communication	L'axe de communication est le message directeur à partir duquel les messages et les moyens de communication seront déclinés. Que voulez-vous dire à vos clientèles cibles? Que souhaitez-vous qu'elles retiennent? Qu'est-ce qui les motivera à adhérer? Pour les organisations publiques, la motivation première pourrait être la mise en place de pratiques rigoureuses et la volonté d'agir en amont afin d'éviter que des situations problématiques ne se concrétisent. Les axes de communication seraient alors **Rigueur et Prévenir plutôt que guérir**.

Stratégie de communication	Maintenant que l'on sait ce que l'on veut dire et à qui, comment va-t-on le dire? C'est dans le cadre de l'établissement de la stratégie que l'on déterminera comment informer et influencer les clientèles cibles. Dans cette partie, vous devez expliquer brièvement comment vous allez communiquer avec elles et décrire les raisons de vos choix ainsi que les moments forts de la démarche : « Quand enclencherez-vous chaque étape? Quelles seront les durées de chacune de celles-ci?, etc. » La stratégie répond à la question « Comment? ». Une attention particulière doit être portée à la communication interne. Les employés de l'organisation constituent votre premier public. S'ils sont bien informés, ils deviendront vos ambassadeurs ; dans le cas contraire, vous laisserez place à la rumeur, qui favorisera les oppositions au projet.
Messages-clés	Les messages-clés constituent un aperçu des principaux messages à transmettre pour atteindre les objectifs fixés. Ils doivent s'adresser aux différentes clientèles déjà identifiées. Ces messages visent à les informer d'abord, mais également à les convaincre. Exemple de messages-clés : ▲ Les citoyens du Québec sont en droit de s'attendre à une gestion rigoureuse des fonds publics. ▲ Les techniques de gestion des risques ont démontré leur efficacité afin d'éviter que des événements indésirables ne se produisent. ▲ La gestion des risques à l'intégrité est une pratique exemplaire qui nous permettra d'améliorer la robustesse de nos processus et de nos décisions.
Échéanciers	Quelles seront les échéances du plan de communication? Quelles seront les dates de début et de fin prévues pour chaque étape de la mise en place? Quels moyens seront utilisés pour mettre en œuvre la stratégie définie (utilisation de l'intranet et d'Internet, conférences-midi, communiqués de presse, matériel graphique, etc.)?
Budget	À cette étape, on doit définir quelles seront les ressources nécessaires à la mise en œuvre de la stratégie et en évaluer les coûts. Il faut tenter d'être aussi précis que possible et mettre en parallèle les dépenses et les échéanciers. Une bonne planification évitera les dépassements imprévus.

Évaluation

Comment évaluerez-vous l'atteinte des objectifs fixés? Il faut définir les indicateurs et la façon dont vous allez obtenir les données. Certains indicateurs seront plus qualitatifs, tels que le degré de rétention des messages par les diverses clientèles. Il faudra alors prévoir un sondage auprès d'un échantillon de clients et le traitement des données ainsi obtenues. D'autres seront quantitatifs et plus faciles à interpréter ; il faudra cependant être en mesure de les comparer aux objectifs fixés.

Vous devez énumérer les outils que vous développerez en vue de mesurer non seulement l'atteinte des objectifs de communication, mais également la pertinence et l'efficacité de l'axe de communication, des messages et des moyens de communication que vous avez employés. Les leçons apprises vous permettront d'améliorer vos performances futures en matière de communication.

Les avantages d'un plan de communication interne et externe efficace sont les suivants :

- faciliter la transmission et l'échange d'information à tous les échelons de l'organisation ainsi qu'avec les fournisseurs, clients et partenaires externes;
- aider à définir le contexte organisationnel et le contexte propre à la gestion des risques à l'intégrité;
- identifier des parties prenantes qui ne l'auraient pas été autrement;
- favoriser la consultation des diverses parties prenantes, tant à l'interne qu'à l'externe;
- mieux comprendre et prendre en compte les intérêts et les points de vue des parties prenantes;
- contribuer à l'étape de l'identification des risques;
- inclure la préoccupation au niveau des communications dans toutes les étapes du projet;
- améliorer les chances de réussite et diminuer les résistances au changement.

ANNEXE 3

Exemples de zones de risques à l'intégrité

Gestion des ressources humaines	▲ Favoritisme (recrutement, processus de dotation, promotion, etc.); ▲ Traitement inéquitable des employés (attribution de dossiers, d'aires de bureau, etc.); ▲ Abus du pouvoir discrétionnaire des gestionnaires; ▲ Divulgation d'actes répréhensibles; ▲ Gestion inadéquate de l'assiduité (feuilles de présence, longueur des pauses, heures de dîner, contrôle inadéquat des employés qui travaillent dans des sites éloignés, etc.); ▲ Rapports de dépenses et de remboursements gonflés; ▲ Non-respect de la confidentialité et conservation non sécuritaire des documents et de l'information; ▲ Discrimination; ▲ Lacunes en matière de professionnalisme, de performance au travail et de formation continue; ▲ Non-respect de la propriété et de l'intégrité intellectuelles; ▲ Utilisation inappropriée des réseaux sociaux; ▲ Appropriation et utilisation du matériel de l'État à des fins personnelles, etc.
Acquisition de biens et services	▲ Proximité avec les fournisseurs, les partenaires privés et les consultants (invitations, cadeaux, fixation et paiement des honoraires, etc.); ▲ Ensemble du processus d'octroi des contrats (trafic d'influence, pots-de-vin, conflits d'intérêts avérés ou apparence de conflits d'intérêts, vol ou substitution de ressources, collusion, fraude); ▲ Passage rapide du secteur public au secteur privé (après-mandat) ou vice versa; ▲ Lobbyisme, etc.

Relations avec les parties prenantes	▲ Relation directe avec la clientèle (usagers, étudiants, parents, demandeurs, etc.); ▲ Difficultés de gestion des clientèles difficiles; ▲ Traitement inéquitable des clients; ▲ Situation de tension avec un partenaire ou un demandeur insatisfait; ▲ Non-respect des valeurs et des pratiques du partenaire; ▲ Non-respect des biens des partenaires; ▲ Non-respect de la propriété intellectuelle du partenaire; ▲ Non-respect des renseignements confidentiels et du secret professionnel dans les relations avec les parties prenantes; ▲ Discrimination; ▲ Iniquité dans la livraison de services; ▲ Mauvaise qualité du service; ▲ Non-respect du citoyen; ▲ Pots-de-vin; ▲ Conflits d'intérêts (ou apparence de conflits d'intérêts); ▲ Acceptation de cadeaux, de repas, de marques d'hospitalité, d'invitations, etc.
Gouvernance	▲ Liens avec les autorités politiques; ▲ Pouvoir discrétionnaire des gestionnaires; ▲ Confusion par rapport à la mission de l'organisation; ▲ Absence ou faiblesse de la reddition de comptes quant à l'utilisation des fonds publics; ▲ Manque de neutralité politique ou de réserve; ▲ Fonctions incompatibles (travail de fonctionnaire versus travail à l'extérieur de la fonction publique, services communautaires ou bénévolat et activités caritatives en conflit avec la mission de l'organisation, collecte de fonds, etc.); ▲ Manque de loyauté; ▲ Lobbyisme, etc.

ANNEXE 4

Principaux risques à l'intégrité liés à la gestion des contrats publics

L'analyse des meilleures pratiques démontre qu'il existe quatre phases critiques dans le processus de gestion des contrats publics. Chacune de ces phases est elle-même constituée d'activités qui sont les étapes obligatoires pour la réalisation de la phase. En fonction de leur domaine d'activités, les organisations constateront qu'il peut y avoir davantage d'activités constituantes, pour chacune de ces phases, que celles qui sont énumérées ci-après.

Les figures 10, 11, 12 et 13 qui suivent présentent en détail chacune de ces phrases.

La phase préparatoire se situe en amont de l'appel d'offres. Elle est généralement composée des activités d'évaluation des besoins, des études d'opportunités, de la conception et de la préparation des plans et devis (cahier de charges).

La phase d'adjudication : Cette phase est constituée de l'appel d'offres, de l'appréciation des offres reçues et de l'adjudication du contrat. Les règles et pratiques établies par le Secrétariat du Conseil du trésor doivent être appliquées rigoureusement à chacune des étapes de cette phase. À cet égard, on peut consulter la Directive concernant la gestion des contrats publics d'approvisionnement, de services et de travaux de construction des organismes publics.

La phase de mise en œuvre : La phase de mise en œuvre est généralement constituée des activités de gestion des contrats, de contrôle des travaux, des activités liées au paiement. Pour certaines organisations, il est possible qu'une phase de mise en service et d'exploitation vienne s'ajouter aux phases déjà mentionnées. Dans ce cas, il est recommandé de reprendre le processus d'analyse des risques et des impacts, car chacune de ces étapes sera normalement constituée de nouveaux contrats, par exemple pour le déneigement, l'éclairage, le surfaçage, l'entretien, etc.

La phase de fermeture : Finalement, la phase de fermeture comprend l'évaluation du bien ou du service, la clôture administrative et la liquidation des contrats.

Figure 10
Phase préparatoire

Activités
en amont de l'appel d'offres

- Évaluation des besoins
- Choix des solutions
- Planification et budgétisation
- Description techique
- Plans et devis, cahier de charges

Indices d'un risque

- Mauvaise évaluation des besoins, de la planification ou des budgets
- Influence d'intervenants internes ou externes
- Imprécisions des éléments techniques ou dans les cahiers de charges
- Irrégularités dans le choix de la procédure
- Imprécisions dans les calendriers de réalisation et leur application inégale selon les soumissionnaires

Plusieurs facteurs peuvent expliquer les raisons pour lesquelles de mauvaises évaluations des besoins sont présentes dans le processus de gestion des contrats publics. On peut d'abord penser qu'il s'agit d'un manque de connaissances ou de compétences de la part des personnes chargées de cette évaluation. Cependant, il est également possible que ces évaluations erronées ou surévaluées soient effectuées volontairement dans le but d'induire certains soumissionnaires en erreur ou d'en favoriser d'autres. Il en va de même pour la planification des travaux, les échéanciers et les budgets.

Il est possible que les personnes qui réalisent les évaluations soient influencées par des acteurs externes qui ont intérêt à ce que l'information soit erronée ou dévoilée à certains soumissionnaires seulement, leur donnant ainsi un avantage concurrentiel important. L'influence pourrait provenir du niveau politique, dans le but de financer un parti ou des activités partisanes. Il ne faut pas oublier que les élus sont, de par leur fonction, des cibles recherchées par les « corrupteurs ».

Des imprécisions volontaires dans le cahier de charges ou dans les éléments techniques d'un contrat peuvent avoir une très grande influence sur l'évaluation de la soumission et donner ainsi des avantages indus à certains soumissionnaires.

Des irrégularités dans le choix des procédures de réalisation des travaux peuvent entraîner une augmentation importante des coûts ou du montant des soumissions. Enfin, des imprécisions dans les calendriers de réalisation peuvent faire augmenter les montants qu'exigent certains soumissionnaires qui n'auraient pas accès à de l'information privilégiée.

Pour chacun de ces effets de la corruption et pour ceux qu'il vous sera possible d'identifier dans cette phase préparatoire à l'octroi des contrats publics, il sera nécessaire de trouver des mesures d'atténuation qui feront diminuer, voire disparaître, leurs répercussions sur les contrats.

Figure 11
Phase d'adjudication

Activités

- Appel d'offres
- Évaluation des offres
- Attribution du contrat

Indices d'un risque

- Critères de sélection destinés à un seul soumissionnaire
- Clauses floues ou ambiguës
- Absence de critères de décision objectifs
- Inefficacité des contrôles lors de l'attribution
- Conflits d'intérêts et corruption au stade de l'évaluation

Lors de la phase d'adjudication, plusieurs risques de corruption peuvent être présents, parfois en simultané.

Les critères de sélection peuvent être tellement précis en matière de compétence ou d'équipement spécialisé qu'il n'y a pas de concurrence possible, puisqu'un seul soumissionnaire répond aux critères énoncés.

Dans certains cas, les clauses de l'appel d'offres sont volontairement floues ou ambiguës, dans le but de préparer les conditions futures de corruption pendant les phases subséquentes.

L'inefficacité des structures de contrôle lors de l'attribution du contrat peut ouvrir la porte à des manipulations. Il peut également y avoir défaut de transparence, par exemple des soumissions qui ne sont pas ouvertes publiquement. Enfin, l'absence ou le choix de la pondération des critères peuvent aussi influencer le processus d'adjudication.

Dans certains cas, les adjudicateurs peuvent conjointement décider, volontairement ou par ignorance, de passer outre les procédures prescrites d'adjudication, ce qui ouvre la porte à toutes sortes de manipulations et d'iniquités.

La divulgation d'information confidentielle concernant la procédure d'adjudication, les critères d'évaluation, le processus de surveillance ou les contenus techniques ou financiers des soumissions divulguées à des concurrents dans le but de favoriser l'un d'eux constitue un risque important qui doit être atténué.

Les conflits d'intérêts et la corruption touchant les personnes responsables de l'évaluation ou de l'attribution des contrats sont au nombre des risques de la phase d'adjudication. Ainsi, un ou des évaluateurs établissent des liens, au fil des ans, avec des fournisseurs et, en échange de cadeaux ou de sommes d'argent, ils favorisent ces derniers lors de l'évaluation.

Certains soumissionnaires peuvent tenter de manipuler les règles du libre marché et faire de la collusion pour favoriser l'un d'entre eux.

Figure 12
Phase de mise en oeuvre

Activités	Indices d'un risque
▲ Gestion des contrats	▲ Mauvaise gestion, clauses contractuelles floues
▲ Contrôle de qualité	▲ Contrôle de qualité déficient (volontaire ou involontaire)
▲ Autorisation de paiement	▲ Autorisation de paiement pour des services ou produits non livrés

Les risques de corruption sont nombreux à la phase de mise en œuvre, particulièrement au niveau de la gestion du contrat. Par exemple, l'insuffisance des contrôles relatifs à la qualité et au calendrier peut avoir des conséquences importantes en augmentant les délais de livraison, ce qui entraîne une augmentation des coûts. La substitution d'un produit par un autre de moindre qualité ou dont la quantité est différente de celle prévue au contrat aura pour conséquence d'augmenter significativement les profits du soumissionnaire.

De plus, le vol d'équipement ou de marchandise avant leur inscription au fichier des actifs du contrat peut faire augmenter les coûts rapidement.

Le défaut de surveillance ou la collusion entre les agences chargées d'effectuer ces contrôles et les sous-traitants sont également des risques à atténuer.

Les autorisations de paiement peuvent être données pour de fausses factures portant sur des biens ou des services non livrés ou encore sur des paiements effectués avant échéance.

Figure 13
Phase de fermeture

Activités	Indices d'un risque
▲ Évaluation	▲ Évaluation positive pour des travaux non effectués ou de qualité inférieure à celle escomptée
▲ Clôture administrative	▲ Autorisation de paiement pour des biens ou services non livrés
▲ Liquidation et clôture des contrats	▲ Autorisation de travaux supplémentaires (avenant)
	▲ Surfacturation

Finalement, à la phase de fermeture du contrat, il existe des risques importants de corruption lors de l'évaluation de conformité. La fermeture administrative peut également être l'occasion d'effectuer de fausses écritures comptables, des transferts de coûts entre contrats ou de la fausse ou de la double facturation de biens ou de services non fournis.

ANNEXE 5

Risques associés à l'emploi ou à la personne

Les risques associés à des comportements non éthiques, voire corrompus, peuvent se développer ou exister à deux niveaux.

Le premier niveau est lié à l'emploi vulnérable ou stratégique en raison de sa nature ou des responsabilités qui y sont associées. Le second est lié à la personne qui occupe un emploi stratégique ou à des responsabilités décisionnelles associées à des processus situés en zone de risques à l'intégrité, telle la gestion de contrats.

L'évaluation des fonctions et des emplois

Avant de déterminer les vérifications de vulnérabilité nécessaires au regard des différentes fonctions et emplois de l'organisation, il importe de déterminer le degré de sensibilité de ceux-ci ainsi que les caractéristiques sécuritaires objectivement requises en lien avec l'emploi ou les responsabilités qui y sont associées.

Une analyse détaillée et des rencontres avec des personnes occupant ces postes ou des postes semblables permettront de bien définir le niveau de sensibilité pour chacun des postes sensibles.

À cette fin, une analyse rigoureuse, intègre et transparente permettra de répondre aux besoins de sécurité, tout en garantissant à l'organisation que les contraintes de gestion ainsi que les dispositions de la Charte des droits et libertés de la personne sont respectées.

L'évaluation de la probité des personnes

Parmi les mesures d'atténuation des risques éthiques ou de corruption liés à la personne, la vérification de probité, pour les personnes occupant des fonctions stratégiques, demeure une mesure préventive pertinente.

Par exemple, le Secrétariat du Conseil du trésor veille à ce que les personnes impliquées dans les processus d'octroi de contrats pour les ministères et organismes aient fait l'objet d'un examen de leur probité. Cependant, rien n'oblige une municipalité à faire de même. Bien que la Loi sur les contrats des organismes publics prévoie qu'une entreprise ou une municipalité voulant conclure un contrat avec des organismes publics ou les municipalités doivent au préalable obtenir une autorisation de contracter avec l'État, rien n'est prévu au niveau des personnes dont l'emploi comporte des responsabilités stratégiques qui peuvent les rendre vulnérables à la corruption.

Il peut en aller de même pour les personnes en position de décider dans d'autres processus situés en zone de risques.

Différents corps policiers québécois et des agences de sécurité privées peuvent offrir un service de vérification aux ministères et organismes qui identifient un besoin de vérification de la probité des personnes.

.

ANNEXE 6

Tableau des risques identifiés (1)

Situation à risque		Contexte du risque		Appréciation du risque		Risque brut
Description de l'activité	Description du risque	Éléments déclencheurs/ Causes	Préjudices potentiels/ Conséquences sur les parties prenantes	Probabilité de matérialisation (1 à 5)	Impact (1 à 5)	Inacceptable (16 à 25) Moyen (5 à 15) Faible (1 à 4)

ANNEXE 7

Tableau des risques identifiés (2)

Risque brut		Contrôles contributifs	Risques résiduels	Évaluation des mesures			Mise en œuvre
Inacceptable (16 à 25) Moyen (5 à 15) Faible (1 à 4)	Tendances futures > = <		Inacceptable Moyen Faible	Stratégies (Accepter Atténuer Transférer)	Échéanciers	Coûts	Responsable

ANNEXE 8

Grille d'aide à la décision éthique

COMPRENDRE LA SITUATION

Quel est le contexte qui amène le questionnement éthique du demandeur?

Marche à suivre	Réponses
Il s'agit d'indiquer les principaux enjeux de la situation et les questions en suspens. Ceux-ci correspondent aux faits marquants de la situation et non pas à l'évaluation qui est faite, ni à des conclusions hâtives. Le répondant peut se demander, par exemple, s'il s'agit d'un dilemme récurrent.	

Est-ce un problème éthique? Sinon, vers quelles ressources puis-je diriger le demandeur?

Marche à suivre	Réponses
Le répondant doit s'assurer qu'il fait face à un véritable dilemme éthique.	

Quelles sont les personnes impliquées dans ce dilemme?

Marche à suivre	Réponses
Plusieurs personnes peuvent être impliquées dans un dilemme, dont l'organisation, l'État, les fournisseurs, les citoyens, les clients, la population en général, les employés et les collègues, les syndicats, les groupes de consommateurs, les groupes environnementaux, les communautés locales, les groupes d'intérêts, les médias, les générations futures, etc. L'éthique intervient toujours dans une situation où le résultat n'est pas automatiquement noir ou blanc, bon ou mauvais. On y fait appel quand il y a des zones grises qui entraîneront nécessairement des conséquences négatives sur les autres, peu importe la décision spontanée. La délibération doit permettre d'aboutir à un résultat où le négatif est minimisé ou encore à des mesures tempérées et équitables pour l'ensemble des parties visées. En déterminant qui y gagnera et qui y perdra, on voit se profiler l'ampleur de la tension qui existe dans la prise de décision.	

Est-ce que le répondant peut consulter une personne-ressource ou un comité pour l'aider à résoudre son dilemme?

Marche à suivre	Réponses
Le répondant peut inciter le demandeur à essayer de trouver des ressources, dans son organisation, qui pourraient l'aider à résoudre son dilemme.	

Est-ce que le répondant peut consulter une personne-ressource, un autre répondant ou un comité pour aider le demandeur à résoudre son dilemme?

Marche à suivre	Réponses
Le répondant peut toujours consulter d'autres personnes, dans son entourage, pour l'aider à réfléchir sur le dilemme qui lui est présenté. Cela dit, il est très important, avant de faire ces consultations, de s'assurer que le demandeur est d'accord pour que le répondant consulte d'autres personnes à ce sujet.	

Comment puis-je formuler le dilemme éthique du demandeur?

Marche à suivre	Réponses
La formulation le dilemme d'action qui se pose dans la situation donnée constitue le point de départ qui permettra par la suite de faire ressortir les valeurs en conflit dans la situation. Il s'agit ici de formuler le dilemme de façon claire, simple et précise.	

Est-ce que je suis en conflit d'intérêts si j'exerce mon rôle-conseil dans ce dilemme? Est-ce que je suis en conflit de rôle? Si oui, vers quelles ressources puis-je rediriger le demandeur?

Marche à suivre	Réponses
Le répondant ne peut se permettre d'être dans une situation de conflit d'intérêts. Puisque le répondant peut assumer plusieurs mandats dans son organisation, il doit s'assurer d'éviter les conflits entre ses différents rôles après avoir formulé clairement le dilemme.	

IDENTIFIER LES ÉLÉMENTS NORMATIFS

Est-ce qu'un ou plusieurs des articles 4 à 12 de la Loi sur la fonction publique s'appliquent?

Est-ce qu'un ou plusieurs des articles 1 à 14 du Règlement sur l'éthique et la discipline dans la fonction publique s'appliquent?

Quels sont les aspects de la brochure intitulée L'éthique dans la fonction publique québécoise qui touchent le dilemme du demandeur?

Quels sont les autres éléments normatifs qui touchent le dilemme du demandeur?

Est-ce que mon organisation a un code d'éthique qui traite du dilemme?

Si la demande touche un membre d'un ordre professionnel visé par le Code des professions, est-il tenu de respecter un code d'éthique ou de déontologie professionnelle?

Marche à suivre	Réponses
Il s'agit ici de faire l'inventaire des normes qui régissent le travail des membres d'une organisation afin de déterminer ce qu'une personne, en l'occurrence un agent public, doit faire dans une situation donnée si elle souhaite agir en conformité avec ces normes. Dans un premier temps, il faut déterminer les dispositions légales, réglementaires et déontologiques qui indiquent le comportement à adopter dans les circonstances. Dans un deuxième temps, il s'agit de connaître les normes qui, sans être écrites, s'appliquent dans le milieu, donc la culture organisationnelle. Certaines normes ou façons de faire qui relèvent de la morale et des mœurs sont imposées par toute culture organisationnelle. Dans certains cas, elles ont préséance sur d'autres dans la décision, car elles renvoient à l'appartenance au groupe et au désir d'identité et de conformité avec celui-ci. Dans un troisième temps, le répondant s'assure d'examiner l'ensemble des codes de conduite, codes d'éthique ou codes de déontologie.	

DÉFINIR LES VALEURS

Quelles sont les valeurs organisationnelles que le demandeur doit prendre en considération dans sa décision?

Marche à suivre	Réponses
Rappelons d'abord que, dans le contexte de la prise de décision, une valeur est quelque chose d'important qui sert de critère pour évaluer si une action peut être considérée comme meilleure qu'une autre. Les valeurs font intervenir la dimension affective d'une décision. Les décisions les plus difficiles à prendre sont celles où la personne est troublée par deux ou plusieurs valeurs, ou encore par des valeurs qui entrent en conflit avec des normes. Le répondant doit faire ressortir ces éléments pour mieux comprendre la nature même du dilemme éthique. Cela dit, d'autres valeurs que celles de l'organisation peuvent être en conflit, comme des valeurs personnelles. C'est également à cette étape que l'on dégage celles-ci.	

Est-ce que ces valeurs sont en conflit? De quelle façon?

Marche à suivre	Réponses
Il faut ensuite déterminer, parmi les valeurs qui ressortent, celles qui engendrent le principal conflit de valeurs, donc les valeurs qui ont le plus de poids dans la décision finale. Rappelons que décider, en éthique, c'est choisir entre deux ou plusieurs valeurs et, en bout de piste, choisir la finalité de l'action. Le répondant peut donc demander pourquoi une valeur a priorité sur une autre dans le dilemme et dans quel contexte l'établissement des priorités quant aux valeurs pourrait changer.	

ANALYSER LES OPTIONS

Quels sont les choix qui s'offrent au demandeur pour résoudre son dilemme?

Marche à suivre	Réponses
Pour pouvoir parler véritablement de décision, il faut que la personne ait à choisir, parmi les différentes possibilités, celle qui lui semble la plus adaptée à l'objectif poursuivi. Pour s'assurer de bien faire le tour de la question, le demandeur doit être conscient de tous les choix, même ceux qu'il ne souhaite pas.	

Quelles sont les conséquences probables, négatives ou positives, de ces choix?

Marche à suivre	Réponses
Il est important pour le demandeur de bien comprendre toutes les conséquences de ses choix, aussi minimes soient-elles.	

Quelle est la meilleure option?

Marche à suivre	Réponses
Le choix de la meilleure option constitue la fin de la réflexion. C'est la dernière étape avant l'action. « La décision est l'aboutissement d'une analyse, d'une réflexion individuelle ou collective nourrissant une délibération, pour arrêter et choisir des actions à réaliser[7]. »	

7 MACCIO, Charles. Exercer une responsabilité, Paris, Chronique sociale, 2001.

DÉCIDER DE L'ACTION

Quelle argumentation et quelle stratégie de communication ont mené à la décision?

Marche à suivre	Réponses
La décision étant prise, le demandeur doit être capable de comprendre comment il est parvenu à la prendre. Il doit bien récapituler son cheminement. La délibération précédente est un outil qui permettra au demandeur de répondre de façon rationnelle de sa décision et, par conséquent, d'en être responsable. C'est également le moment pour le répondant de revenir, avec le demandeur, sur la décision spontanée présentée précédemment. Cela permet de constater dans quelle mesure la délibération a conduit le demandeur à nuancer sa position de départ, voire à la changer, si celui-ci constate, au cours du processus, que cette position était plus problématique qu'il ne le croyait ou qu'elle avait des effets plus dommageables sur les autres que ce qu'il aurait pensé au départ.	

Le demandeur est-il capable de défendre sa décision devant des collègues, des citoyens, des partenaires ou des médias?

Marche à suivre	Réponses
Cette étape est un exercice intéressant pour le demandeur, puisqu'elle permet de « tester » sa décision avec un regard extérieur et, en fin de compte, de peaufiner son argumentation et de réaffirmer la légitimité de celle-ci.	

ANNEXE 9

Avis éthique

Cette section permettra au répondant d'utiliser une méthode simple pour rédiger un avis éthique.

Rappelons d'abord que la rédaction d'un avis éthique est un travail de recommandation, et non de décision. Mentionnons également que l'avis éthique n'est pas un avis juridique. Sa visée n'est donc pas d'examiner la conformité aux normes légales. Le mandat du répondant doit être clair à cet égard et connu de ceux qui lui demanderont un avis éthique. Le répondant doit plutôt s'interroger sur l'action ou la décision qui est la plus juste dans les circonstances, en se souciant des personnes concernées. L'éthique, il faut le rappeler, consiste à faire des choix judicieux et à décider avec justesse dans l'incertitude du moment.

Dans son avis, le répondant doit donc s'interroger sur certaines règles ou façons de faire, s'il constate ou observe que leur application dans la pratique pose des interrogations, ou qu'elle cause des malaises ou des tensions chez le personnel ou une autre partie prenante (citoyens, partenaires, fournisseurs, etc.). Il doit clarifier en quoi certaines actions soulèvent un problème par rapport aux valeurs organisationnelles. Parfois complémentaire à l'avis juridique, l'avis éthique pose un regard particulier et nouveau sur une situation. Il permet de mettre en lumière le problème en cernant les valeurs qui sont en jeu et en s'interrogeant sur la finalité recherchée par la décision ou l'action.

L'avis éthique est donc une démarche de réflexion qui suppose une prise de conscience des risques et des dilemmes éthiques, qu'ils soient potentiels, apparents ou réels, associés à une décision ou à une action dont on a demandé l'évaluation éthique. Le répondant a alors le mandat d'identifier ces risques et dilemmes éthiques, d'évaluer leur probabilité ainsi que l'ampleur des inconvénients qui pourraient découler de ceux-ci. L'avis éthique est donc de nature prospective, en ce sens qu'il prend forme dans la réflexion et qu'il a toujours comme leitmotiv l'intérêt public.

Le guide suggéré ici est une adaptation de celui que propose le Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information. Il ne doit donc pas être considéré comme un modèle unique, mais plutôt comme un moyen de faciliter et de guider la réflexion. Il peut être adapté aux circonstances et aux particularités d'une organisation[8].

Guide pour la rédaction d'un avis éthique

Délimitation du rôle du répondant

- Le demandeur de l'avis comprend-il le rôle du répondant?
- S'agit-il d'un avis éthique?
- Quels sont les objectifs de la demande d'avis?
- Quelles sont les conditions de la rédaction de l'avis?
- Quelle est la portée de l'avis?
- Le répondant est-il en conflit d'intérêts ou en conflit de rôle au sujet de l'avis?

8 SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES ET À L'ACCÈS À L'INFORMATION, Direction de l'accès à l'information et de la protection des renseignements personnels. Guide de référence – Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, 2008.

Délimitation du thème

- Qui sont les personnes ou groupes de personnes à consulter pour aider à la rédaction de l'avis?
- Quelle est la documentation pertinente à consulter sur le sujet?
- Quels sont les autres types de renseignements à recueillir?
- Quels sont les liens entre la mission de l'organisation et le sujet de l'avis?

Parties prenantes

- Qui est touché (directement ou indirectement) par l'avis (personnes, organisations, population, etc.)?

Définition des enjeux éthiques

- Quels sont les dilemmes ou risques éthiques en cause, s'il y a lieu?
- Quel est le contexte?
- Quels sont les facteurs déclencheurs ou aggravants?
- Quelle est la probabilité que de tels dilemmes ou risques surviennent, et à quelle fréquence?

Réflexion sur les normes et les valeurs

- Quelles sont les normes déontologiques qui touchent le sujet de l'avis?
- Quelles sont les valeurs touchées par le sujet de l'avis?
- Quel est le conflit de valeurs, s'il y a lieu?
- Comment puis-je interroger les valeurs qui sous-tendent les décisions et les actions qui sont au cœur de l'avis?

Réflexion sur les recommandations

- Quelles sont les recommandations visant la prévention des risques éthiques?
- Quels sont les grands axes de réflexion qu'il est indispensable d'aborder dans les recommandations?
- Quelles sont les recommandations visant la résolution des conflits de valeurs?
- Quels seront les effets, positifs ou négatifs, de chacune des recommandations?

Rédaction des recommandations

- Quelles sont les recommandations finales?
- Quel est le délai proposé pour la mise en place des recommandations?
- Quels sont les moyens nécessaires à la mise en place des recommandations?
- Les recommandations doivent-elles être diffusées?
- Quelles sont les études ou analyses supplémentaires que pourrait faire le répondant à ce sujet?
- Après la remise de l'avis aux autorités, quel est le rôle du répondant?

ANNEXE 10

Gabarit de plan de gestion des risques à l'intégrité

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance

ANNEXE 11

Modèle de plan de prévention des risques à l'intégrité

Afin d'aider les organisations à préparer leur plan de prévention des risques à l'intégrité, nous proposons un modèle qui contient l'information de base nécessaire à la préparation d'un plan efficace. Les organisations devront, en fonction de leur contexte, adapter ce modèle en y ajoutant les éléments propres à leur situation.

La direction

Résultats attendus **(ce que nous voulons réaliser)**	**Activités que nous faisons déjà** **(politiques, programmes, instructions, etc.)**	**Actions planifiées** **(ce que nous ferons pour atteindre nos objectifs)**	**Responsable**	**Échéance**
Les hauts dirigeants et les cadres supérieurs sont directement impliqués dans l'implantation du plan de gestion de prévention à l'intégrité.	Les codes de conduite et les attentes signifiées aux cadres supérieurs contiennent des objectifs clairs de prévention de la corruption et des dérapages éthiques.	Une formation obligatoire à l'intention de tous les gestionnaires, laquelle inclura la promotion de l'intégrité, de la culture éthique et la prévention de la corruption.		
	Les descriptions de fonction des cadres supérieurs incluent la responsabilité de prévenir toute forme de corruption.	Le choix des personnes qui occuperont des emplois de cadre inclura des critères d'évaluation de l'intégrité.		
	Les évaluations périodiques incluent des mesures de performance concernant leur implication dans le domaine de la prévention et le contrôle de la corruption et de la culture éthique.	Le système de reconnaissance inclura des éléments relatifs à la prévention de la corruption et à la promotion des comportements éthiques.		

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
La prévention de la corruption fait partie de toutes les autres activités, planification stratégique, plan d'affaires et plans d'audit interne.	Tous les gestionnaires de l'organisation contribuent à l'identification des emplois et processus vulnérables à la corruption dans les secteurs qui sont sous leur responsabilité.	Les meilleures pratiques en matière de prévention de la corruption et en éthique seront mises en commun et on en discutera lors des réunions de planification stratégique.		

Les codes de conduite

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
L'organisation possède un code de conduite qui reflète ses valeurs, ses dispositions déontologiques et ses normes éthiques, remis à tous les employés.	Le code de conduite est disponible sur le site Internet de l'organisation.	La première révision du code de conduite sera réalisée en consultant tous les cadres et gestionnaires, qui, à leur tour, consulteront tous les employés.		
	On discute du code lors des réunions avec les employés.			
	Le code est présenté lors de l'embauche et les chefs d'équipe ou les gestionnaires revoient les normes avec les employés lors des évaluations périodiques.			

Les politiques, les procédures et les systèmes de contrôle

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
Les opérations de l'organisation sont contrôlées sur la base de politiques claires au sujet de la prévention de la corruption. Les procédures et les systèmes de contrôle incluent des indicateurs de vulnérabilité qui sont contrôlés régulièrement.	Les politiques de gestion de la vulnérabilité à la corruption sont revues annuellement et le nom du responsable et sa fonction sont clairement identifiés.	Les gestionnaires seront encouragés à informer le responsable de la révision de la politique de gestion s'ils identifient des failles dans les processus de contrôle.		

Les systèmes de gestion

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
Les systèmes informatiques de l'organisation sont robustes et répondent aux normes de sécurité. Ils incluent des mesures de contrôle de la corruption.	Des processus d'autorisation rigoureux sont en place pour l'accès aux banques de données.	Des lecteurs de caractéristiques physiques seront mis en place pour contrôler les accès.		
Les vérifications internes.	Le Service de la vérification interne est proactif dans le développement de programmes de vérification et de détection de la corruption, particulièrement dans les secteurs les plus à risque.	Des critères d'évaluation des secteurs les plus à risque seront élaborés et l'identification des emplois les plus vulnérables sera réalisée au cours de la prochaine année.		

Les divulgations internes

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
On encourage et facilite la divulgation interne de comportements déviants et on enquête à leur sujet.	Un système confidentiel de divulgation a été mis en place.	Un sondage sera réalisé afin de connaître la perception des employés au sujet du processus de divulgation.		
		Des sessions de sensibilisation seront offertes aux employés.		
		La Direction des ressources humaines fera de la sensibilisation auprès des nouveaux employés.		
		Un processus de divulgation par l'entremise du site intranet sera mis en place et une campagne d'information sera menée afin d'en assurer la compréhension.		

La réponse à la corruption

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
Le plan de gestion de la vulnérabilité est revu systématiquement chaque année et des modifications ou ajouts sont apportés afin d'en assurer l'efficacité.	Un plan initial de gestion de la vulnérabilité est en cours de préparation.	Assurer la mise en place des mesures identifiées dans le plan. La révision systématique du plan pour en assurer l'efficacité sera effectuée au moment du rapport annuel de gestion.		
Des sanctions disciplinaires sont imposées dans les cas de manquements au code de conduite.	Le code de conduite contient des articles en référence aux actes répréhensibles et à la mauvaise gestion.	Un guide de référence sera élaboré afin de guider les gestionnaires.		

La formation

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
Les employés qui œuvrent dans des secteurs identifiés comme étant vulnérables à la corruption reçoivent de la formation sur la corruption, sur ses répercussions, sur sa détection ainsi que sur les pièges à éviter.	Une formation de base est donnée aux employés lors de leur entrée en fonction.	Assurer la participation des employés à l'identification des activités à risque.		
		Assurer la formation continue des employés sur les nouveaux stratagèmes employés et sur la façon de les déceler.		

Les personnes-ressources

Résultats attendus (ce que nous voulons réaliser)	Activités que nous faisons déjà (politiques, programmes, instructions, etc.)	Actions planifiées (ce que nous ferons pour atteindre nos objectifs)	Responsable	Échéance
Des personnes-ressources, appelées des répondants, sont formées et disponibles pour répondre aux questions des employés au sujet de la corruption sous toutes ses formes et de l'éthique.	Une formation de relayeur a été élaborée.	De la formation continue sera donnée aux relayeurs pour assurer que leurs connaissances sont à jour.		

BIBLIOGRAPHIE

Documents en langue française :

BARTOLI, Annie et al. « Les défis éthiques de la recherche académique : le cas de la France et des États-Unis », Revue française d'administration publique, nº 140, 2011, p. 659-667.

BARTOLI, Annie et al. « Vers un management public éthique et performant », Revue française d'administration publique, nº 140, 2011, p. 629-639.

BOISVERT, Yves. « Éthique et gestion publique : apprendre des scandales », Revue française d'administration publique, nº 140, 2011, p. 641-658.

CONSEIL DU TRÉSOR. Politique de gestion contractuelle concernant la conclusion des contrats d'approvisionnement, de services et de travaux de construction des organismes publics, Québec, 2014.

DUSSAULT, René et Louis BORGEAT. Traité de droit administratif, 2e édition, Tome II, Québec, Les presses de l'Université Laval, 1986.

ISO. Guide 73 – Management du risque – Vocabulaire, Genève, International Organization for standardization, 2009.

ISO. ISO 31 000 – Management du risque – Principes et lignes directrices, Genève, International Organization for standardization, 2009.

KOS, Drago. « Combattre la corruption pour rétablir la confiance », Paris, L'Annuel de l'OCDE 2014, p. 73-74.

MACCIO, Charles. Exercer une responsabilité, Paris, Chronique sociale, 2001.

MICHAUD, Nelson et al. Secrets d'États? Les principes qui guident l'administration publique et ses enjeux contemporains, 2011.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES. Confiance à l'égard des pouvoirs publics : Données concrètes, politiques et prise de décision – Un programme d'action pour l'avenir, Paris, Conseil de l'OCDE, 2013.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES. Les composantes de l'intégrité : Données et références pour le suivi des évolutions au sein des administrations publiques, Paris, Comité de la gouvernance publique, 2008.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES. Recommandation du conseil sur l'amélioration du comportement éthique dans le service public incluant les principes propres à favoriser la gestion de l'éthique dans le secteur public, Paris, Conseil de l'OCDE, 1998.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES. Vers un cadre pour l'intégrité solide : Instruments, processus, structures et conditions de mise en œuvre, Paris, Forum mondial sur la gouvernance publique, 2009.

ORGANISATION DES NATIONS UNIES. Office contre la drogue et le crime, Convention des Nations Unies contre la corruption, Vienne, 2004.

SECRÉTARIAT À LA RÉFORME DES INSTITUTIONS DÉMOCRATIQUES ET À L'ACCÈS À L'INFORMATION, Direction de l'accès à l'information et de la protection des renseignements personnels. Guide de référence – Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, 2008.

SECRÉTARIAT DU CONSEIL DU TRÉSOR. Guide de vérification du processus de gestion contractuelle, Québec, 2014.

UNION EUROPÉENNE. Rapport de la Commission au Conseil et au Parlement européen, Rapport anticorruption de l'UE, Bruxelles, Commission européenne, 2014.

Documents en langue anglaise :

BRITISH STANDARDS INSTITUTION. Risk management – *Code of practice and guidance for the implementation* of BS ISO 3100, London, 2011.

INDEPENDENT COMMISSION AGAINST CORRUPTION. *Corruption Risks in NSW Government Procurement – The management Challenge*, Sydney, 2011.

JOINT AUSTRALIAN NEW ZEALAND INTERNATIONAL STANDARD ; ISO 31000: 2009. *Risk Management - Principles and Guidelines*, Sydney et Wellington, 2010.

MCPHEE, Ian. *Risk and Risk Management in the Public Sector,* Canberra, Australian National Audit Office, Public Sector Governance and Risk Forum, 2005.

NEW SOUTH WALES AUDIT OFFICE. *Managing Risk in the NSW public sector*, Sydney, 2002.

NEW SOUTH WALES LEGISLATIVE ASSEMBLY, Public Accounts Committee. *Risk Management in the NSW Public sector*, Sydney, 2005.

NEW SOUTH WALES TREASURY. *Internal Audit and Risk Management Policy*, Sydney, 2009.

NEW SOUTH WALES TREASURY. *Risk Management Toolkit for NSW Public Sector Agencies – Executive Guide*, Sydney, 2012.

NEW SOUTH WALES TREASURY. *Total Asset Management Risk Management Guideline*, Sydney, 2004.

OECD, *Risk Management and Corporate Governance*, Paris, OECD Publishing, 2014.

OFFICE OF QUALITY IMPROVEMENT. *Facilitator Tool Kit – A Guide for Helping Get Results*, Madison, University of Wisconsin Board of Regents, 2007.

OLAYA, Juanita. *Integrity Pacts in Public Procurement – An Implementation Guide*, Berlin, Transparency international, 2013.

PROJECT MANAGEMENT INSTITUTE. *A guide to the project management body of knowledge* (PMBOK guide), Pennsylvania, 2013.

ROWE, Elizabeth et al. *Organised crime and public sector corruption: A crime scripts analysis of tactical displacement risks in Trends & Issues in Crime and criminal justice*, Canberra, Australian Institute of Criminology, no 444, 2013.

STATE OF VICTORIA. *Managing Risk across the Public Sector*, Melbourne, Victorian Auditor General Office, 2004.

TAYLOR-GOOBY, Peter et Jens O. ZINN. *Risk in Social Science*, Oxford University Press, 2006, p. 22-26.

Document en langue espagnole :

REPÚBLICA DE COLOMBIA. *Guía para la administración del riesgo*, Bogotá, Departamento administrativo de la Función pública, 2011.

Secrétariat
du Conseil du trésor
Québec