DE LA CONNAISSANCE À LA MAÎTRISE DES RISQUES DANS LES COLLECTIVITÉS LOCALES

ifaci
institut français de l'audit et du contrôle internes

GROUPE PROFESSIONNEL
COLLECTIVITÉS TERRITORIALES

La présente publication a pour objet d'actualiser et compléter le contenu d'un numéro des Cahiers de la Recherche de l'IFACI publié en mai 2006 sous le titre « L'audit interne et le management des collectivités territoriales - La cartographie des risques »

Elle prend appui sur les importantes avancées méthodologiques obtenues dans ce domaine et sur l'observation des bonnes pratiques dans les collectivités déjà engagées dans une démarche assurantielle de contrôle et de management des risques.

CONTRIBUTEURS

Coordination :

Stéphane Labonne - Région des Pays de la Loire

Ont contribué à sa rédaction :

- Alexis de Perier - Grenoble Ecole de Management
- Léo-Paul Karle - Ville de Marseille
- Anne-Fabienne Malet - Ville et Eurométropole de Strasbourg
- Nathalie Pasquet - Ville et Eurométropole de Strasbourg
- Alexandra Tay - Département de Seine Saint-Denis
- Franck Villot - Département du Morbihan
- Olivier Watel - Département du Pas-de-Calais

Ont contribué à son amélioration en tant que relecteurs :

- David Gaudry - Région Auvergne Rhône-Alpes
- Julien Blondeau - Métropole de Lille
- Bruno Borodine - Région Bretagne
- Adeline Galli-Bacculini - Département des Alpes Maritimes
- Marie-France Nansot - Métropole de Lyon
- Sébastien Passion - Département de la Manche
- Martial Prévalet - Département du Doubs
- Raphael Szary - Région Ile-de-France

METHODOLOGIE

La présente publication est le fruit d'un travail collaboratif associant deux Groupes Professionnels de l'IFACI et la Conférence des Inspecteurs et auditeurs territoriaux (CIAT).

Les Groupes Professionnels de l'IFACI ont pour objectif d'échanger sur des thématiques spécifiques d'un secteur d'activité, d'un domaine, ou d'une fonction.

Ces échanges peuvent, le cas échéant, faire l'objet de publications destinées aux auditeurs et contrôleurs internes du secteur concerné.

Ces publications sont réalisées sous la responsabilité des membres du Groupe de travail, et leur contenu technique n'engage ni les organisations auxquels appartiennent les participants de ce Groupe, ni l'IFACI.

Le travail de rédaction a été mené sous la supervision du Groupe Professionnel « Collectivités Territoriales » de l'IFACI

Le Groupe Professionnel « Collectivités Territoriales » de l'IFACI a pris l'initiative du chantier et a fourni l'équipe en charge de sa conduite.

Les points de divergence résiduels ont été mis en discussion au sein de la Conférence des Inspecteurs et auditeurs territoriaux

La Conférence des Inspecteurs et auditeurs territoriaux (CIAT) a été sollicitée pour apporter une expertise sur les points techniques demeurés en discussion au sein du groupe de travail.

Ces éléments ont été présentés dans le cadre d'un Atelier dédié[1] tenu dans le cadre des 12èmes Journées nationales des Inspecteurs et auditeurs territoriaux les 14 et 15 octobre 2021 ; les solutions ici adoptées sont conformes aux conclusions obtenues par consensus.

Le Groupe Professionnel « Contrôle interne » de l'IFACI a procédé à une relecture finale

En dernier lieu, le Groupe Professionnel « Contrôle interne » de l'IFACI a réalisé une relecture du texte consolidé et y a apporté différentes modifications qui sont intégrées à la présente version.

Ces propositions ont permis d'enrichir la démarche méthodologique et les ressources techniques présentées avec la valeur ajoutée que donnent des regards croisés et complémentaires sur une même recherche de gain de sécurité et d'efficacité dans des environnements marqués par une complexité croissante.

[1] Cet Atelier intitulé « De la connaissance à la maîtrise des risques - Présentation de la mise à jour des Cahiers de la Recherche IFACI » a totalisé 26 participants issus de 18 collectivités

INTRODUCTION 9

1 Des collectivités confrontées à un contexte complexe, volatil, incertain et ambigu 11

1-A Les enjeux et objectifs d'une démarche assurantielle globale 11

1-A-1 La conformité 13

1-A-2 L'efficacité et efficience de la gestion 24

1-A-3 La transparence et la qualité du reporting 25

1-B Donner une assurance raisonnable de l'atteinte de ces objectifs 31

1-B-1 Eléments de méthodologie 33

1-B-2 Les acteurs 38

1-B-3 Les instances de pilotage et de suivi 47

2 Les prérequis d'une démarche de management des risques 48

2-A Les conditions du succès 51

2-A- 1 Evaluer l'environnement externe 51

2-A - 2 Evaluer l'environnement interne 52

2-B Choisir un mode opératoire 57

2-B-1 Trouver la meilleure entrée pour l'identification des risques 58

2-B-2 Collecter et agréger les données disponibles 61

2-B-3 Déterminer le périmètre de l'exercice 61

3 Passer en phase opérationnelle 66

3-A Etablir le portefeuille des risques de la collectivite 68

3-A-1 Recenser les risques 68

3-A-2 Regrouper les risques 75

3-A-3 Evaluer et hiérarchiser les risques 76

3-A-4 Etablir un cadre de gouvernance approprié 82

3- B- Construire une démarche assurantielle globale 83

3-B-1 Les outils et ressources nécessaires 88

3-B-2 Piloter et optimiser les mesures de maîtrise 93

CONCLUSION 99

Glossaire 102

Fiches techniques 111

Fiche technique 1 113

Cadre réglementaire des collectivités territoriales en matière de déontologie et de prévention des conflits d'intérêts .....

Fiche technique 2 126

Recommandations de l'Agence française anti-corruption relatives à la prévention et à la détection des actes contraires à la probité .....

Fiche technique 3 140

Obligations liées à la mise en œuvre des financements de la politique européenne de cohésion ....

Fiche technique 4 146

Expérimentation de la certification des comptes dans les collectivités locales (2017-2023) .....

Fiche technique 5 152

Mode opératoire pour la mise en place d'un système de management de la continuité d'activité ..

Fiche technique 6 157

Le processus de management du risque .....

Fiche technique 7 159

Les trois lignes de maîtrise des risques .....

Fiche technique 8 162

Profils engagés dans une démarche de management et de maîtrise des risques - Acteurs en charge de la gouvernance .....

Fiche technique 9 165

Profils engagés dans une démarche de management et de maîtrise des risques- Acteurs en charge des trois lignes de maîtrise .....

Fiche technique 10 180

Risques le plus fréquemment rencontrés et exemples d'univers de risques dans différents types de collectivités .....

Fiche technique 11 184

Outils & méthodes d'évaluation des risques présentés dans la Norme ISO 31000 relative au management des risques.....

Fiche technique 12 209

Exemples d'échelles de criticité des risques.....

Fiche technique 13 215

Proposition pour la mise en place d'une échelle de maîtrise des risques.....

Fiche technique 14 218

Normes professionnelles de l'audit interne .....

Fiche technique 15 222

Rôle de l'audit interne dans le management des risques .....

Fiche technique 16 225

Le tableau MARCI comme outil de pilotage des audits.....

Fiche technique 17 227

Exemple de Fiche synthétique de suivi et de traitement d'un risque (criticité & maitrise).....

Bibliographie..... 249

Sources utilisées pour le présent ouvrage..... 250

Lectures complémentaires recommandées..... 251

INTRODUCTION

L'épisode de crise sanitaire qui a durement marqué l'actualité depuis le printemps de l'année 2020 montre la grande volatilité de l'environnement institutionnel et économique dans lequel s'inscrit l'action des collectivités territoriales.

Or et tout particulièrement dans ces périodes de grande incertitude, les collectivités doivent être garantes de la continuité des services essentiels qu'elles délivrent à la population mais également de la disponibilité des moyens nécessaires, notamment dans le cadre de Plans de continuité d'activité, pour accompagner les acteurs du développement, faciliter leur rebond ou stimuler l'émergence d'opportunités nouvelles.

Pour relever ce défi important, il leur revient d'intégrer à leur fonctionnement une démarche d'identification et d'anticipation des risques principaux propre à fonder une assurance raisonnable quant à la poursuite de leurs missions en toute circonstance et à la préservation d'un service de qualité rendu au meilleur coût.

Le travail de fond requis pour créer cette dynamique nouvelle et la maintenir sur le long terme relève de fonctions complémentaires qui se déploient progressivement dans les collectivités : le manager des risques, le responsable du contrôle interne et le responsable de l'audit interne.

La présente publication se propose de présenter les interactions entre ces différentes fonctions et d'exposer les étapes conduisant à une sécurisation des objectifs stratégiques et opérationnels de la collectivité auprès des élus, des agents mais également des citoyens et des usagers.

Elle prend appui sur les travaux déjà menés dans ce domaine et en particulier sur les Cahiers de la Recherche de l'Institut français de l'audit et du contrôle internes (IFACI) publiés en mai 2006 avec pour titre « *L'audit interne et le management des collectivités territoriales - La cartographie des risques* ».

Ces éléments doivent cependant être réexaminés au regard des mutations à l'œuvre et des enseignements tirés des expérimentations en cours.

Il convient également de tenir compte de la montée en puissance de nouveaux modes de gouvernance fondés sur les principes d'équité, d'intégrité et de transparence.

Ces exigences montantes apparaissent dans le nouvel objectif des organisations d'atteindre une situation d'*accountability* qui peut se traduire par la recherche d'une « bonne gouvernance » par le biais de méthodes de gestion tournées vers davantage de transparence et de lisibilité de l'administration.

Pour rendre compte de pratiques diverses mais convergentes et illustrer l'étroite articulation des métiers du contrôle interne, de l'audit interne et du management des risques, le choix a été fait d'un ouvrage collectif sollicitant la contribution d'auditeurs, de contrôleurs internes et de managers des risques issus de collectivités de tous horizons.

De par son objet et sa composition, la Conférence des inspecteurs et auditeurs territoriaux est l'instance la mieux habilitée pour réunir cette équipe pluridisciplinaire ; le partenariat noué avec l'IFACI a permis en outre de consolider l'assise méthodologique des travaux conduits.

Notre propos n'est pas de dresser une feuille de route pour la mise en place d'une démarche de management des risques qui s'appliquerait dans tous les cas de figure et moins encore de proposer une boîte à outils standardisée assortie d'un manuel de montage universel.

Les pages qui suivent ont pour ambition de fournir des éléments d'argumentaire et des pistes d'action pour initier ou consolider la co-construction d'un modèle de management fondé sur l'anticipation et le pilotage stratégique en réponse à un environnement complexe autant qu'incertain.

Ces propositions s'adressent à l'ensemble des collectivités territoriales, sans considérer leur taille ou leur nature, tant il apparait que toutes sont confrontées aux mêmes enjeux de continuité, de transparence et de confiance pour agir efficacement dans leurs périmètres respectifs.

Bien entendu, chaque collectivité ou groupement de collectivités engagée dans une démarche de management des risques sera amenée à y affecter des moyens humains et matériels proportionnés à ses capacités et à ses besoins.

Il peut être ainsi opportun de procéder par étape graduelle et de prendre appui pour les premières étapes sur les fonctions support existantes, sans qu'il soit immédiatement nécessaire de mobiliser des ressources additionnelles dédiées.

Ce parti pris de progressivité et de pragmatisme peut être un gage de pérennité du changement attendu dans la mesure où il permet de gagner plus aisément l'adhésion des différentes parties engagées en créant une dynamique de conviction et de résultats tournée vers la réalisation d'un objectif ambitieux.

Il reflète également la situation générale des collectivités.

Une enquête réalisée dans le courant de l'année 2018 par l'Agence française anti-corruption auprès de l'ensemble des entités du Service public local a ainsi montré que moins de 2 % d'entre elles étaient dotées d'une cartographie des risques, cette proportion étant portée à 30 % pour les régions et 8 % pour les départements.

De même, 30 % des collectivités répondantes ont déjà mis en place un dispositif de contrôle interne, ce pourcentage atteignant 85 % dans le cas des régions, 76 % pour les communes de plus de 80 000 habitants et 67 % pour les départements.

Enfin, 5 % des collectivités ayant participé à l'enquête déclarent avoir créé une fonction d'audit interne, cette part n'étant significative que dans les régions (70 %), les départements (62 %) et les communes de plus de 80 000 habitants (38 %).

Il est bien évident que ces chiffres n'ont pas vocation à être inversés du jour au lendemain mais tout concourt à ce qu'ils progressent sensiblement et le présent ouvrage n'ambitionne qu'à y aider.

1 Des collectivités confrontées à un contexte complexe, volatil, incertain et ambigu

L'environnement institutionnel, économique et social attaché aux politiques nationales et locales n'est plus seulement imprévisible, il est devenu plus volatil, incertain, complexe et ambigu.

De par leurs missions de service public et leur ancrage territorial, les collectivités n'échappent pas à ce contexte influençant fortement leurs enjeux et leurs objectifs prioritaires.

En réponse, elles sont amenées à déployer une démarche assurantielle reposant sur l'identification des principaux risques inhérents à leur fonctionnement et sur la mise en place des mesures de maîtrise appropriées et efficientes.

Cette démarche vise à connaître, anticiper et maîtriser les menaces pesant sur la continuité de service et la bonne fin des politiques dont elles ont la charge ; elle permet également de mieux identifier et exploiter les opportunités qui y sont associées, comme pendant et contrepartie d'une dynamique de changement à l'œuvre sur leurs différents leviers d'action.

1-A Les enjeux et objectifs d'une démarche assurantielle globale

Chaque collectivité est appelée à déterminer un ensemble de dispositifs nécessaires à la maîtrise du fonctionnement de ses activités.

Choisis par l'encadrement et mis en œuvre par les responsables positionnés tout au long de la chaîne hiérarchique, ces dispositifs sont destinés à fournir une assurance raisonnable quant à la réalisation des objectifs de la collectivité.

Il est proposé de regrouper ces objectifs en trois grandes catégories, en conformité avec la nomenclature du référentiel COSO de contrôle interne.

Le premier objectif que doit remplir une collectivité touche à la **conformité** (voir Section 1-A-1).

On désigne par là le respect des lois et règlements applicables à la collectivité ainsi que la correcte exécution des obligations contractuelles ou conventionnelles auxquelles elle est tenue.

Le second objectif à atteindre concerne **l'efficacité et l'efficience de la gestion** (voir Section 1-A-2).

Il s'agit notamment des objectifs de performance opérationnelle et financière, ainsi que de sauvegarde du patrimoine de la collectivité comprenant les actifs, les agents et l'image de la collectivité ; ils sont mesurés au regard de l'efficacité et de l'efficience des opérations menées.

Un troisième objectif recouvre **la transparence et la qualité du reporting** (voir Section 1-A-3).

Cette dernière catégorie recouvre la qualité du reporting interne et externe, financier et extra-financier ; celle-ci est notamment évaluée selon la fiabilité des procédures de collecte, le respect des délais fixés, la transparence et la traçabilité des données fournies.

L'assurance raisonnable susceptible d'être apportée à l'Exécutif et à la Direction générale portera prioritairement sur les chances de réalisation de ces objectifs ; elle dépendra notamment de la pertinence et de l'efficacité du dispositif de contrôle interne mis en œuvre par la collectivité.

Le référentiel COSO de contrôle interne

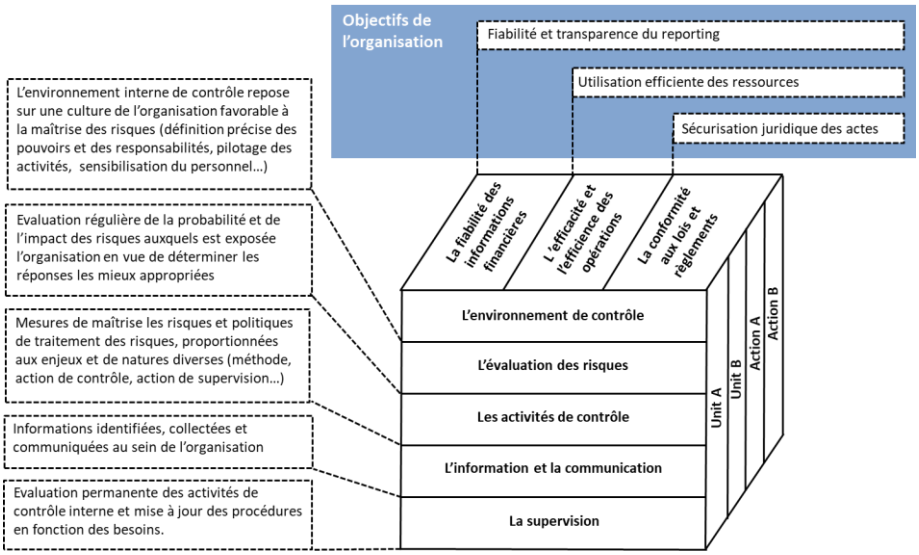
Le COSO[2] est un référentiel de contrôle interne qui a tout d'abord été conçu pour limiter les tentatives de fraudes dans les rapports financiers des entreprises. Il a ensuite évolué vers un processus de contrôle interne fondé sur l'évaluation et le pilotage des risques qui a pour but de mettre toute organisation en situation de maîtriser ses activités et d'atteindre ses objectifs.

Le dispositif d'évaluation et de contrôle ainsi mis en place permet de fournir une assurance raisonnable quant à la réalisation des objectifs liés aux opérations, au reporting et à la conformité.

Le référentiel COSO suggère une vision en trois dimensions du management des risques :

- trois objectifs sont poursuivis (conformité aux lois et aux règlements, l'efficacité et l'efficience des opérations, la fiabilité des informations financières) ;
- cinq composantes du contrôle interne permettent l'atteinte de ces objectifs (l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, la supervision) ;
- chaque niveau de l'organisation est tenu de contribuer à l'évaluation des risques et de mettre en œuvre les mesures de maîtrise appropriées, dans son champ de responsabilité particulier.

Cette approche intégrée et pluridimensionnelle est généralement représentée dans le **Cube COSO**



L'utilisation du référentiel COSO s'est étendue avec l'obligation faite aux sociétés américaines cotées de mettre en œuvre des règles de transparence et de bonne conduite en rapport avec les attentes de leurs investisseurs et actionnaires (loi Sarbanes-Oxley de 2002).

Ces dispositions ont été introduites en France par la loi n°2003-706 du 1er août 2003 - dite loi de Sécurité Financière - et tendent à se renforcer depuis lors.

[2] COSO est l'acronyme pour Committee of Sponsoring Organisation of the Treadway Commission, une organisation à but non lucratif qui a établi une définition standardisée du contrôle interne et créé un cadre pour évaluer son efficacité

Préalablement à la mise en place d'une démarche assurantielle globale, une collectivité doit ainsi identifier avec précision les objectifs qu'il lui revient d'atteindre dans chacune des trois catégories susmentionnées.

Bien entendu, les obligations respectives des collectivités peuvent sensiblement différer selon leurs périmètres d'action, l'importance de leurs engagements contractuels et conventionnels et plus généralement les arbitrages pris par les exécutifs élus ; de la même façon, des prescriptions nouvelles sont susceptibles d'être apportées notamment du fait de changements intervenus dans la législation en vigueur ou de la survenance d'événements brutaux et fortement disruptifs - comme la crise sanitaire - qui seraient de nature à altérer durablement la continuité de service voire même à affecter les leviers nécessaires à la conduite de certaines politiques essentielles.

Par-delà cette diversité des situations existantes et de leur caractère évolutif, il est néanmoins possible d'identifier un bloc d'obligations partagées entre l'ensemble des collectivités et ajustables au regard de leurs trajectoires et contraintes particulières.

Pour aider à reconnaître et mesurer ce socle commun, un examen rapide des trois grandes catégories d'objectifs précédemment citées s'impose.

1-A-1 La conformité

La conformité constitue l'un des trois grands objectifs qu'une collectivité est tenue d'atteindre.

On peut même considérer qu'il s'agit de l'objectif qui doit être prioritairement réalisé du fait des conséquences juridiques pour la collectivité et ses représentants attachées au non-respect des obligations issues de la législation applicable ou de tout engagement contractuel ou conventionnel envers des tiers.

Conformité au cadre législatif et réglementaire

Les lois de décentralisation successives à partir des « lois Defferre » de 1982 et 1983 ont conféré aux collectivités territoriales des compétences plus nombreuses et ceci dans des secteurs plus diversifiés.[3]

Depuis l'année 2000, ces textes sont consolidés dans le Code général des collectivités territoriales (CGCT) qui définit le cadre et les modalités de fonctionnement des structures publiques locales.

Un simple parcours de ce code permet de prendre la mesure des objectifs de conformité pour une collectivité, lesquels s'élèvent encore si l'on y ajoute les textes applicables à ses champs d'intervention particuliers (Code de l'urbanisme, Code de l'action sociale et des familles, Code de l'environnement…).

[3] Institut français de l'audit et du contrôle internes (Éd.). (2006). L'audit interne et le management des collectivités territoriales : La cartographie des risques. IFACI.

En tout dernier lieu, le Code général de la fonction publique [4] a été créé dans le but de consolider les textes législatifs et réglementaires traitant des droits et obligations des agents publics ainsi que des questions de déontologie, notamment :

- les lois dites « Le Pors » :
  - la loi n° 83-634 du 13 juillet 1983, portant droits et obligations des fonctionnaires, communes aux trois fonctions publiques,
  - la loi n° 84-16 du 11 janvier 1984, la loi n° 84-53 du 26 janvier 1984 et n° 86-33 du 9 janvier 1986, portant dispositions statutaires relatives, respectivement, à la fonction publique de l'Etat, à la fonction publique territoriale et à la fonction publique hospitalière.
- la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires,
- la loi n° 2019-828 du 6 août 2019 de transformation de la fonction publique.

La mise en application de ce code est fixée au 1er mars 2022 pour sa partie législative[5]

La profusion de ces obligations peut conduire à leur non-application totale ou partielle, par méconnaissance des normes applicables ou erreur dans l'interprétation qu'il convient d'en donner.

Les recommandations émises par les Chambres régionales des comptes lors de leurs contrôles permettent ainsi de passer en revue les différentes fragilités potentielles ou avérées de sa collectivité en matière de conformité, qu'il s'agisse de la gestion des ressources humaines, de l'achat public, de la tenue de la comptabilité ou de la situation patrimoniale.

Pour illustrer ce propos, il est proposé de traiter en particulier quatre sujets éminemment transversaux que sont la sécurité et la protection des travailleurs, le bon usage des deniers publics, les atteintes à la probité et la protection des données à caractère personnel.

Ces thématiques croisent d'autres obligations réglementaires auxquelles les collectivités sont exposées ; leurs sources sont multiples mais on peut notamment relever le Code de la commande publique, le Code de la construction et de l'habitation, le Code de l'urbanisme et le Code civil.

Dans leurs champs d'application respectifs, ces textes concourent à une gestion vertueuse et efficiente de la chose publique, qui doit être un but également partagé entre les agents et les élus.

En conséquence, la conformité aux normes applicables n'est pas un exercice qui trouve sa justification en lui-même mais doit bien plutôt s'entendre comme une étape nécessaire pour atteindre des standards plus élevés quant à la performance de l'organisation et sa transparence vis-à-vis des citoyens et usagers.

[4] L'ordonnance n° 2021-1574 du 24 novembre 2021 portant partie législative du Code général de la fonction publique a été publiée au JORF le 5 décembre 2021

[5] Une partie règlementaire est également prévue pour 2023

Ressorts et enjeux d'une démarche globale de compliance

Un nombre croissant de collectivités s'engagent dans une démarche de compliance couvrant les différents aspects de leurs activités et visant à créer une dynamique vertueuse tournée vers la probité et l'exemplarité publiques.

La notion de compliance désigne une politique globale de connaissance, de maîtrise et de traitement des risques de gestion (financiers, réglementaires, anti-corruption…) au moyen d'outils préventifs et détectifs appropriés.

Plus largement, la mise en œuvre d'une telle démarche implique un investissement politique et managérial au plus haut niveau répété sur une durée longue :

« *Au-delà des outils et procédures qui peuvent être ponctuellement mis en place, la compliance appelle tout à la fois un engagement et un pilotage stratégiques, une culture interne de la bonne gestion, une volonté permanente*. »[6]

Pour s'assurer de l'adhésion de tous et ancrer solidement cette culture nouvelle dans les pratiques de la collectivité un cheminement par étape est recommandé.

A cet égard, les points d'attention suivants peuvent être considérés comme autant de gages de succès et pérennité des actions menées :

- procéder à un recensement exhaustif des obligations réglementaires et légales pesant sur la collectivité puis formaliser les dispositifs mis en place en réponse à ces obligations, ceux-ci devant être valorisés comme des outils de compliance déjà effectifs ;
- consolider en continu ce travail dans une bibliothèque des procédures qui permettra de vérifier l'homogénéité des modalités de contrôle et de traitement en vigueur et aussi d'identifier les obligations non encore traitées ;
- établir une cartographie des risques de non-conformité afin de prioriser les actions correctrices à mener et de mesurer les progrès réalisés en la matière [7] ;
- mettre en place des lignes directrices ou de guides de bonne conduite dans le but de déterminer précisément les comportements et attitudes attendus des élus ou des agents dans des situations à risque préalablement décrites. ;

Plus généralement, il est recommandé de veiller à une stricte proportionnalité entre les moyens mobilisés et les enjeux afférents, de manière à faire prévaloir des solutions simples, économes en ressources et immédiatement opérationnelles.

[6] Samuel Dyens « La compliance, une politique globale de gestion des risques au sein de l'action publique » La Gazette - 3 juin 2019

[7] Voir pour plus de détails l'article de Samuel Dyens « La cartographie des risques, outil central de la compliance publique » - Actualité juridique des collectivités locales - Octobre 2018

i. Sécurité et protection des travailleurs

Conformément aux dispositions des articles L 4121-1 à L. 4121-3 du Code du travail issues de la loi n° 91-1414 du 31 décembre 1991, chaque employeur, public ou privé, est tenu de prendre les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs dont il a la charge.

Cette exigence d'ordre général se décline en trois thématiques :

- assurer la sécurité et protéger la santé physique et mentale des travailleurs,
- mettre en œuvre les principes généraux de prévention des risques professionnels,
- procéder à l'évaluation des risques.

Les articles R 4121-1 à R. 4121-4 du Code du travail fixent un cadre opératoire commun répondant à des principes de cohérence, facilité d'appropriation et traçabilité.

Il est ainsi demandé à l'employeur de transcrire et de mettre à jour dans un document unique les résultats de l'évaluation des risques pour la santé et la sécurité des travailleurs.

Dans cette optique, les risques s'analysent comme la « *combinaison de la probabilité de la survenue d'un ou plusieurs événements dangereux ou expositions à un ou à de tels événements et de la gravité du préjudice personnel ou de l'atteinte à la santé que cet événement ou cette / ces exposition(s) peuvent causer*. »[8]

Il revient à l'autorité territoriale d'initier, décider et organiser la prévention de ces risques, en tant que responsable de la sécurité et de la protection de la santé des agents qu'elle emploie.

Cette tâche incombe en premier lieu à la Direction générale, dans la mesure où il est de sa responsabilité de donner des consignes de travail appropriées aux tâches à effectuer et aux risques inhérents, de mettre en place des règles d'hygiène et de sécurité proportionnées et de vérifier leur correcte application.

La Direction générale peut en outre prendre appui sur :

- un assistant / conseiller de prévention qui a pour rôle de participer à la politique de prévention et d'évaluation des risques ;
- un Agent Chargé de la Fonction d'Inspection (ACFI) chargé de contrôler les conditions d'application des règles d'hygiène et de sécurité ainsi que d'émettre des recommandations pour l'amélioration des dispositifs existants ;
- des organismes extérieurs qualifiés tels que la Caisse d'assurance retraite et santé au travail (CARSAT), des bureaux de contrôle, l'Inspection du travail, des formateurs, des experts (ergonomes…)

De même, les instances représentatives réunies au sein du Comité technique contribuent à la protection de la santé et de la sécurité des agents dans leur travail ; elles sont ainsi systématiquement consultées sur les règlements et consignes en matière d'hygiène et de sécurité du travail.

[8] Norme OHSAS 18001 Management de la santé et la sécurité au travail

ii. Bon usage des deniers publics

L'exigence de bon usage des deniers publics recouvre à la fois l'absence de toute utilisation frauduleuse et la mise en œuvre des diligences nécessaires à la prévention de comportements négligents dans l'attribution ou le suivi des aides conduisant à une dilapidation des ressources publiques dédiées.

Cette notion contient donc la lutte contre la fraude - que l'on développera ensuite - mais aussi plus largement la recherche de la qualité et de l'exactitude de la dépense qui doit être strictement proportionnée, mesurée à l'aune du but recherché, justifiée quant aux montants versés et scrupuleusement tracée tout au long de la chaîne de traitement.

En conséquence, la collectivité doit disposer des moyens de maintenir sa trajectoire budgétaire, d'assurer la continuité de service et de mener à bien ses politiques prioritaires dans un cadre de ressources contraint et fortement dépendant de facteurs extérieurs.

Une illustration de cette préoccupation se trouve dans les deux premiers alinéas de l'article L 1611-4 du Code général des collectivités territoriales qui disposent :

« *Toute association, œuvre ou entreprise ayant reçu une subvention peut être soumise au contrôle des délégués de la collectivité qui l'a accordée.*

Tous groupements, associations, œuvres ou entreprises privées qui ont reçu dans l'année en cours une ou plusieurs subventions sont tenus de fournir à l'autorité qui a mandaté la subvention une copie certifiée de leurs budgets et de leurs comptes de l'exercice écoulé, ainsi que tous documents faisant connaître les résultats de leur activité. »

Cette mesure ancienne trouve son origine dans un décret du 30 octobre 1935 relatif au contrôle des associations, œuvres et entreprises subventionnées.

Elle a été renforcée depuis lors, en particulier par la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations qui, dans le troisième alinéa de son article 10, fait obligation aux collectivités d'établir une convention avec tout organisme de droit privé recevant une subvention dépassant le montant de 23 000 euros[9].

Le sixième alinéa du même article prévoit en outre que « *lorsque la subvention est affectée à une dépense déterminée, l'organisme de droit privé bénéficiaire doit produire un compte rendu financier qui atteste de la conformité des dépenses effectuées à l'objet de la subvention* » ; il y est précisé que ce compte rendu financier est déposé « *dans les six mois suivant la fin de l'exercice pour lequel elle a été attribuée* ».

Ces différentes dispositions ont pour objet de faciliter, documenter et homogénéiser le contrôle de la dépense à la charge des collectivités.

A l'inverse, le défaut de contrôle et/ou de conventionnement constitue un risque juridique à part entière.

[9] Ce montant a été fixé par le décret n° 2001-495 du 6 juin 2001

iii. Obligations en matière de détection et prévention des actes d'atteinte à la probité, de libre accès à l'information et de transparence

Des dispositions de plus en plus contraignantes ont été adoptées en matière de prévention des risques de conflits d'intérêts, en commençant avec l'interdiction du cumul sur la même personne des fonctions d'ordonnateur et de comptable public.

Ainsi, l'article L. 2122-5 du CGCT dispose que "*les agents des administrations financières ayant à connaître de la comptabilité communale, de l'assiette, du recouvrement ou du contrôle de tous impôts et taxes, ne peuvent être maires ou adjoints, ni en exercer même temporairement les fonctions dans toutes les communes qui, dans leur département de résidence administrative, sont situées dans le ressort de leur service d'affectation*".

Depuis la mise en place des premières mesures prises dans ce sens - il y a de cela 25 ans - un corpus législatif et réglementaire a été progressivement constitué pour encadrer le fonctionnement des collectivités territoriales et renforcer l'attention donnée aux questions de déontologie et de transparence.

→ Voir **Fiche technique 1**

Cadre réglementaire des collectivités territoriales en matière de déontologie et de prévention des conflits d'intérêts

La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin 2 » invite les collectivités à mettre en œuvre des politiques de long terme en faveur de la probité sur le modèle des acteurs économiques les plus directement exposés à ce type de risque.

Ces politiques prennent la forme d'un plan global anti-corruption et de prévention des atteintes à la probité reposant sur les huit piliers décrits dans l'article 17-II de la loi.

Pour accompagner et faciliter leur déploiement, le même texte a créé une Agence française anticorruption (AFA) sous la forme d'un service à compétence nationale placé auprès du ministre de la Justice et du ministre en charge du Budget.

L'AFA exerce un double rôle de conseil et de contrôle.

Au titre des missions de conseil et sur le fondement du second paragraphe de l'article 3 de la loi, l'AFA émet à échéance régulière des «*recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme*».

Dans un premier avis destiné à « *aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme* » paru au Journal officiel du 22 décembre 2017, l'AFA fixe un ensemble de recommandations pour la mise en place de mesures préventives, détectives et correctives appropriées à chaque situation.

Des indications particulières y sont données pour préciser le contenu des recommandations et en faciliter la mise en application par les acteurs publics.

Une actualisation de ces recommandations a été publiée au Journal officiel du 12 janvier 2021.

Au titre de ses missions de contrôle et en application du troisième paragraphe du même article 3 de la loi, l'AFA évalue «*la qualité et l'efficacité des procédures mises en œuvre au sein (…) des collectivités territoriales* ».

Il est précisé plus loin que ces contrôles donnent lieu à l'établissement de rapports contenant «*les observations de l'agence concernant la qualité du dispositif de prévention et de détection de la corruption mis en place au sein des entités contrôlées ainsi que des recommandations en vue de l'amélioration des procédures existante.*»

S'agissant des collectivités locales, ces contrôles ne sont pas assortis de possibilité de sanction en cas de non-respect des prescriptions fixées.

Toutefois, l'AFA se réserve la possibilité de déférer au juge les actes ou décisions contraires au droit applicable qu'elle serait amenée à relever.

La lutte contre la fraude est ainsi de plus en plus prégnante dans le corpus réglementaire des collectivités et renforce sensiblement leurs enjeux de conformité.

→ Voir **Fiche technique 2**

Recommandations de l'Agence française anti-corruption relatives à la prévention et à la détection des actes contraires à la probité

Vers des obligations accrues sur les collectivités en matière de lutte contre la corruption ?

Le 19 octobre 2021, une proposition de loi visant à renforcer la lutte contre la corruption a été déposée par le député Raphaël Gauvain.

Ce texte a pour objet de reprendre et compléter les dispositions de la loi Sapin 2 à la lumière des cinq années écoulées depuis sa mise en application.

Il prévoit notamment un renforcement de l'engagement des personnes publiques au travers des dispositions suivantes :

- obligation faite à certaines collectivités de mettre en œuvre « *une ou plusieurs des mesures et procédures* » listées dans l'article 17-II de la loi Sapin 2, la définition des mesures à mettre en œuvre par catégorie d'acteur relevant d'un décret ultérieur en Conseil d'État (selon la nature de l'entité et son niveau d'exposition aux risques) ;
- là où il sera rendu nécessaire, présentation annuelle du plan anti-fraude à l'assemblée délibérante afin qu'il fasse l'objet d'un débat public ;
- publication systématique des rapports de contrôle - ou simplement de leurs conclusions - sur le modèle de ceux des cours régionales des comptes.

Une dernière disposition significative touche le transfert au profit de la Haute autorité pour la transparence de la vie publique (HATVP) des fonctions de conseil et de contrôle exercées par l'AFA auprès des collectivités territoriales, ceci afin de créer un pôle national pleinement dédié à l'accompagnement des actions de lutte contre la fraude menées par les acteurs publics[10].

[10] Voir notamment l'article de Fleur Jourdan et Dan Phan « Proposition de loi « Sapin 3 » : vers plus d'obligations et de contrôles sur les acteurs publics » - La Semaine Juridique - Éditions administrations et collectivités territoriales - 29 novembre 2021 (n° 48)

iv. Protection des données à caractère personnel

Le Règlement général pour la protection des données personnelles (RGPD)[11] fixe les modalités de traitement de toute information se rapportant à des personnes physiques identifiées ou identifiables de manière à écarter toute possibilité d'accès ou d'utilisation abusive.

Au sein de chaque collectivité, un Délégué à la protection des données (DPD) est garant de sa correcte application.

Le DPD est chargé du recensement des traitements qui se traduit par la mise en place d'un Registre des traitements des données personnelles dont l'objet est d'assurer la traçabilité de l'ensemble des données personnelles collectées et traitées par la collectivité et ses organismes associés.

Il présente également les mesures de sécurité physiques, organisationnelles et logique pour chacun des traitements concernés.

Il mesure le niveau de risque attaché à chacun des traitements recensés en termes d'impact et de probabilité/fréquence ; pour les risques les plus critiques, il s'assure que sont menées des études d'impact sur la vie privée (PIA - *Privacy Impact Assessment*) en vue de proposer des mesures de remédiation appropriées selon le principe du *Privacy by Design & by default* (pseudonymisation, miniminalisation de la collecte, éloignement des sources de risque…).

De même, il a soin que l'évaluation des risques relatifs aux différents traitements identifiés soit en cohérence avec la cartographie générale des risques de la collectivité.

Il veille également avec le Responsable de la sécurité des systèmes à ce que les mesures de sécurité arrêtées couvrent de manière adéquate les risques encourus.

Sur la base de ces éléments, le DPD vérifie au fil de l'eau les points suivants :

- les traitements de données existants sont correctement renseignés et les registres tenus ;
- le Registre des traitements de données rend compte de la totalité des opérations effectuées ;
- les clauses relatives à la protection des données personnelles sont dûment mentionnées dans les contrats et conventions passés par la collectivité ;
- les cas de traitement nécessitant un consentement des propriétaires des données concernées sont identifiés ;
- le recueil des consentements est effectivement assuré selon ces procédures ;
- les droits individuels à la protection des données et de la vie privée associés à chaque type de traitement sont précisément reconnus et portés à la connaissance des personnes concernées de manière complète et transparente, compréhensive et non équivoque ;
- les données à caractère personnel sont conservées selon les modalités prescrites ;
- les traitements sont sécurisés conformément au Référentiel général de sécurité (RGS) issu de l'ordonnance n° 2005-1516 du 8 décembre 2005.

La Commission nationale de l'informatique et des libertés (CNIL) est habilitée à mener des contrôles tendant à vérifier la correcte application de ces dispositions, sur le fondement de l'article 19 de la loi modifiée n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - Ses dispositions sont entrées en application le 25 mai 2018

Au-delà des objectifs de conformité liés au cadre législatif et réglementaire, une collectivité se doit également d'agir conformément aux engagements contractuels passés avec des tiers publics comme privés.

Pour ce qui concerne les relations avec les organismes de droit privé recevant une aide dépassant un seuil minimal de 23 000 euros, on a vu précédemment que la loi n° 2000-321 du 12 avril 2000 porte obligation pour les collectivités d'établir une convention définissant l'objet, le montant, les modalités de versement, les conditions d'utilisation et les modalités de contrôle et d'évaluation de la subvention attribuée ; ce même texte prévoit que l'organisme bénéficiaire produit un compte rendu financier propre à attester de la conformité des dépenses effectuées à l'objet de la subvention.

Cet outil d'information financière vient utilement renforcer les moyens dont dispose la collectivité pour procéder au contrôle des fonds attribués.

Il répond au cas basique de l'octroi d'une aide contribuant à l'activité d'une structure pour autant qu'elle s'inscrit dans les objectifs poursuivis par la collectivité attributaire.

La mise en œuvre des politiques territoriales sollicite toutefois de multiples autres formes de partenariat institutionnel et économique qui donnent lieu à des montages juridiques et financiers complexes susceptibles d'engager la responsabilité des collectivités, des élus et des agents publics ayant part à la gouvernance, au suivi ou au contrôle des actions menées.

La pleine maîtrise de ces dispositifs et des régimes de responsabilité afférents est un enjeu essentiel d'une démarche assurantielle globale ; elle requiert une attention particulière et amène souvent la collectivité à acquérir une expertise dédiée.

Deux illustrations permettront d'en prendre la mesure.

i. Engagements pris vis-à-vis des satellites

Les organismes partenaires associés - usuellement qualifiés d'organismes satellites - se caractérisent par une contribution soutenue au service public et une dépendance financière significative vis-à-vis des collectivités.

Ces dernières disposent de représentants au sein des organes de décision de ces organismes et exercent un contrôle renforcé pouvant aller jusqu'au contrôle analogue à celui exercé sur leurs propres services pour les entités les plus intégrées.

Ces entités de droit public (syndicat mixte, groupement d'intérêt public, régie autonome…) ou de droit privé (Sociétés d'économie mixte locales, Sociétés publiques locales, Sociétés d'économie mixte à opération unique…) sont liées contractuellement ou par leurs statuts avec la collectivité à laquelle ils sont adossés.

Dans la mesure où il conditionne la production de service public de qualité, le respect des clauses contractuelles ou statutaires est une des garanties de l'atteinte des objectifs stratégiques et opérationnels portés par la collectivité.

Selon leur statut, les risques et le pilotage seront de nature différente.

A titre d'exemple, pour les Sociétés d'économie mixte locales et les Sociétés publiques locales, la réalisation des objectifs et le respect des engagements sont généralement appréciés au travers de l'article L. 1524-5 du CGCT imposant aux « *organes délibérants des collectivités territoriales et de leurs groupements actionnaires, de se prononcer sur le rapport écrit qui leur est soumis au moins une fois par an par leurs représentants au conseil d'administration ou au conseil de surveillance* ».

ii. Engagements pris vis à vis de l'Union européenne

Construite par paliers successifs depuis plus de 30 ans, la politique de cohésion est un *moteur essentiel du projet européen* et trouve logiquement un fort ancrage dans les textes fondateurs des institutions communautaires.

Cette politique répond à la demande de solidarité entre les territoires de l'Union contenue dans les paragraphes 1 et 2 de l'article 174 du Traité sur le fonctionnement de l'Union Européenne[12] :

« *Afin de promouvoir un développement harmonieux de l'ensemble de l'Union, celle-ci développe et poursuit son action tendant au renforcement de sa cohésion économique, sociale et territoriale.*

*En particulier, l'Union vise à réduire l'écart entre les niveaux de développement des diverses régions et le retard des régions les moins favorisée*s. »

A cette exigence première de rattrapage économique et social des territoires les moins favorisés se sont progressivement ajoutées des préoccupations touchant à l'attractivité entrepreneuriale de l'espace européen à l'échelle internationale et à la promotion d'un modèle de développement intelligent, durable et inclusif.

Les programmes de la politique européenne de cohésion sont abondés par des financements dédiés représentant environ 35 % du budget total de l'Union.

Ils sont mis en œuvre sur des périodes pluriannuelles auxquelles sont associées des indicateurs de réalisation permettant d'attester la contribution effective des différents fonds mobilisés à l'atteinte des objectifs stratégiques de l'Union.

Les principaux instruments de la politique de cohésion sont :

- le Fonds européen de développement régional (FEDER) qui permet le remboursement de dépenses d'infrastructure concourant à la compétitivité et à l'attractivité du territoire selon un modèle de croissance tourné vers la Recherche et le développement ;
- le Fonds social européen (FSE/FSE+) qui vise au renforcement des politiques d'inclusion et au renforcement du taux d'emploi de la population active ;
- le Fonds européen agricole pour le développement rural (FEADER) qui a pour objet de favoriser la compétitivité de l'agriculture, de garantir la gestion pérenne des ressources naturelles et la mise en œuvre de mesures en faveur du climat.

En tant qu'acteurs essentiels de ces politiques, les collectivités territoriales sont associées de manière croissante à la mise en œuvre des crédits de la politique européenne de cohésion.

[12] Aussi appelé traité de Rome (25 mars 1957), son appellation actuelle fait suite à la signature du Traité de Lisbonne le 13 décembre 2007

Ainsi en application de l'article 78 de la loi n° 2014-58 du 27 janvier 2014 de modernisation de l'action publique territoriale et d'affirmation des métropoles - dite loi MAPTAM - les régions ont la charge des programmes de la génération 2014-2020 abondés par les crédits du FEDER et les crédits du FSE dédiés aux politiques de formation ainsi que les programmes régionaux de développement rural recevant des crédits du FEADER.

Ces dispositions ont été globalement reconduites pour les programmes de la période 2021-2027 en cours d'examen et d'approbation par la Commission européenne.

Les régions mettent en œuvre ces programmes en tant qu'autorités de gestion de plein exercice et rendent directement compte de la bonne utilisation des fonds alloués auprès de la Commission européenne et, le cas échéant, de la Cour des comptes européenne.

Par ailleurs, de nombreuses autres collectivités - à commencer par les départements - ainsi que certains Etablissements publics de coopération intercommunale bénéficient de financements de la politique de cohésion au titre des politiques dont ils ont la charge par délégation expresse des autorités de gestion ; ils mobilisent ces ressources sous la supervision directe de l'autorité délégataire et contribuent, par les actions qu'ils mènent, aux objectifs du programme considéré.

Or des obligations particulières pèsent sur les Régions au premier chef - en leur qualité d'autorités de gestion de plein exercice - mais aussi sur les collectivités territoriales contribuant à la mise en œuvre des programmes de la politique européenne dans un cadre de gestion déléguée.

En cas d'usage abusif des crédits européens qui leur sont confiés, celles-ci sont notamment passibles de corrections financières forfaitaires en réparation du préjudice causé au budget de l'Union.

En outre, elles doivent justifier de diligences particulières en matière de lutte contre la fraude, conformément à la priorité que s'est donnée l'Union.

→ Voir **Fiche technique 3**

Obligations liées à la mise en œuvre des financements de la politique européenne de cohésion

1-A-2 L'efficacité et efficience de la gestion

Cette catégorie d'objectif renvoie à la capacité d'une organisation à atteindre les objectifs opérationnels qu'elle s'est préalablement fixés, objectifs exprimés en termes d'efficacité socio-économique, de qualité de service et d'efficience de la gestion.

Notion centrale depuis les années 1990 marquées par le New Public Management (NPM) et mise en lumière par la loi organique relative aux lois de finances n° 2001-692 du 1er août 2001 (LOLF), la notion de performance s'est progressivement affirmée pour mieux répondre aux spécificités du secteur public local.

Celles-ci résident notamment dans la nécessaire prise en compte d'une gouvernance publique multi-partenariale, d'une fonction de production double (réalisation de services publics engendrant des externalités positives), de la poursuite entre autres de l'intérêt général et du bien commun, des structures de production multiservices, avec de nombreuses compétences, et des publics à fois bénéficiaires (usager du service public) et ressources (à travers l'impôt et la tarification).

Les évolutions apportées à cette notion ont été notamment étudiées par David Carassus dans un ouvrage de référence intitulé « *Le pilotage des politiques publiques locales, de la planification à l'évaluation* »[13].

A cet égard, il relève que « *la performance publique est caractérisée, dans une logique multidimensionnelle, par la capacité d'une organisation publique à maîtriser ses ressources humaines, financières et organisationnelles, afin de produire une offre de services publics adaptée, en qualité et en quantité, répondant aux besoins de ses parties prenantes et générant des effets positifs sur son territoire* ».

La collectivité se doit ainsi de veiller à la bonne réalisation de ses opérations, en cherchant à les optimiser afin de répondre à ces différents objectifs ; la non-atteinte de cet objectif l'expose en effet particulièrement à des risques stratégiques, politiques et sociétaux pouvant se traduire par de lourdes conséquences financières et juridiques.

La maîtrise des ressources évoquée dans cette définition de la performance publique locale renvoie aux enjeux liés à la sauvegarde des actifs de la collectivité.

Ces enjeux correspondent aux risques inhérents à un défaut de protection des ressources financières, humaines, patrimoniales de la collectivité contre la possibilité de pertes ou de dommages résultant de gaspillage, d'abus, d'une mauvaise gestion, d'erreurs, d'irrégularités ou de fraude.

Pour les collectivités, disposer d'une assurance raisonnable quant à la réalisation des objectifs de sauvegarde des actifs présente une importance accrue pour le secteur public du fait de la provenance des fonds considérés mais également de la fragilité intrinsèque des procédures d'inventaire qui accentue d'autant leur vulnérabilité face à ce type de risques.

Au même titre que les recommandations émises par les Chambres régionales des comptes en matière de régularité, l'examen de celles liées à la performance peuvent s'avérer très instructives.

[13] Edition Berger Levrault ; octobre 2020

1-A-3 La transparence et la qualité du reporting

Cette troisième et dernière catégorie d'objectifs répond principalement aux enjeux de la transparence financière, lesquels reposent sur la fiabilité, la disponibilité, l'intégrité des données nécessaires au pilotage financier et opérationnel des collectivités.

Ce sujet longtemps peu exploré est amené à se renforcer avec les perspectives du compte financier unique et de la certification des comptes.

Une préoccupation omniprésente mais longtemps diffuse

Jusqu'à une date récente, la transparence financière a été faiblement encadrée et laissée à l'initiative des collectivités territoriales et de leurs groupements[14].

Il en a résulté une situation paradoxale dans laquelle des principes fortement affirmés sont en pratique peu appliqués.

Pour autant, l'obligation de transparence à laquelle sont assujetties les administrations publiques locales est indiscutablement au cœur de nos institutions.

Ainsi la Déclaration des droits de l'homme et du citoyen de 1789, qui est partie intégrante du bloc de constitutionnalité, dispose dans son article 14 que « *tous les citoyens ont le droit de* […] *suivre l'emploi* [de la contribution publique] ».

Cet engagement fondateur est ainsi traduit dans les dispositions de l'article 47-2 de la Constitution : « *Les comptes des administrations publiques sont réguliers et sincères. Ils donnent une image fidèle du résultat de leur gestion, de leur patrimoine et de leur situation financière*. »

Le droit à l'information des élus est pour sa part garanti par l'article L.2121-13 du code général des collectivités territoriales (CGCT)[15] en vertu duquel « *tout membre du conseil municipal a le droit, dans le cadre de sa fonction, d'être informé des affaires de la commune qui font l'objet d'une délibération* ».

Le principe de transparence ainsi énoncé va d'ailleurs au-delà du seul accès aux documents administratifs[16] car il vise aussi à rendre accessibles les documents et les données communiqués ou de les rendre publics.[17]

De même, l'article 10 de la loi d'orientation n° 92-125 du 6 février 1992 relative à l'administration territoriale de la République rappelle que « *le droit des habitants de la commune à être informés des affaires de celle-ci et à être consultés sur les décisions qui les concernent, indissociables de la libre administration des collectivités territoriales, est un principe essentiel de la démocratie locale* ».

[14] Le Nocher, B. (2020) « Le paradoxe de la transparence financière dans les collectivités : Un enjeu ancien, une mise en œuvre récente. » https://www.lagazettedescommunes.com/690608/le-paradoxe-de-la-transparence-financiere-dans-les-collectivites-un-enjeu-ancien-une-mise-en-oeuvre-recente/?abo=1

[15] Ce libellé est issu de la loi n° 96-142 du 21 février 1996

[16] L'accès aux documents administratifs est garanti par l'article 1er de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public. Cette loi a été intégrée au Code des relations entre le public et l'administration issu de l'ordonnance n° 2015-1341 du 23 octobre 2015.

[17] Le Nocher, B. (2020). Le paradoxe de la transparence financière dans les collectivités : Un enjeu ancien, une mise en œuvre récente. https://www.lagazettedescommunes.com/690608/le-paradoxe-de-la-transparence-financiere-dans-les-collectivites-un-enjeu-ancien-une-mise-en-oeuvre-recente/?abo=1

Par contraste et jusqu'à un passé récent, peu de dispositions contraignantes garantissaient l'exécution de cette règle commune.

A titre d'exemple, l'article 11 de la même loi fixait en outre le principe d'un débat d'orientation budgétaire dans les communes comptant 3500 habitants et plus ; cette obligation toute formelle a été abrogée par l'article 12 de la loi n° 96-142 du 21 février 1996.

Toutefois, l'article L 2312-1 du CGCT, issu de l'article 93 de la loi du 27 janvier 2014 de modernisation de l'action publique territoriale et d'affirmation des métropoles (MAPTAM), a rétabli l'obligation pour ces mêmes communes et leurs établissements publics administratifs de conduire chaque année un débat « *sur les orientations générales du budget de l'exercice ainsi que sur les engagements pluriannuels envisagés et sur l'évolution et les caractéristiques de l'endettement* ».

De fait, les principales obligations en matière de transparence financière découlaient de l'action des juridictions financières.

L'article L 243-6 du Code des juridictions financières[18] dispose ainsi que le rapport d'observations définitives produit au terme de la procédure d'examen de gestion par la chambre régionale des comptes territorialement compétente doit être communiqué par l'exécutif de la collectivité territoriale à son assemblée délibérante, dès sa plus proche réunion, et donne lieu à un débat.

En outre, l'article L 132-8 du même code prévoit que la Cour des comptes établit chaque année un « *rapport public portant sur la situation financière et la gestion des collectivités territoriales et de leurs établissements publics* » ; ce rapport comprend les résultats des contrôles et enquêtes réalisés par les chambres régionales des comptes, auxquels s'ajoute un rapport public dédié à la situation des finances publiques locales.

Une dynamique forte s'est enclenchée depuis la loi NOTRe du 7 août 2015

A compter de la publication de la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République (dite loi NOTRe) d'importants progrès ont été réalisés en matière de présentation et transparence des comptes qui ont permis de résoudre ce paradoxe dans le sens d'une meilleure information des citoyens et des autres parties prenantes concernées.

Les avancées que l'on doit à cette loi sont de divers ordres.

En premier lieu, son article 107 reprend et renforce les dispositions de l'article 2312-1 du CGCT relatif aux informations données aux élus quant aux orientations budgétaires, aux engagements pluriannuels envisagés ainsi qu'à la structure et la gestion de la dette.

Un décret n° 2016-841 du 24 juin 2016 précise le contenu du rapport d'orientations budgétaires à destination des élus : évolution prévisionnelle des dépenses et des recettes, programmation d'investissement, encours de la dette, structure et évolution des effectifs, éléments sur la rémunération (traitements indiciaires, régimes indemnitaires, avantages en nature…), durée effective du travail… Le décret précise que les orientations budgétaires doivent « *permettre d'évaluer l'évolution prévisionnelle du niveau d'épargne brute, d'épargne nette et de l'endettement à la fin de l'exercice auquel se rapporte le budget* » ; il y est également indiqué que le budget primitif et le compte administratif sont nécessairement accompagnés d'une « *présentation brève et synthétique retraçant les informations financières essentielles* […] *afin de permettre aux citoyens d'en saisir les enjeux* ».

[18] Disposition issue de la loi n° 2008-1091 du 28 octobre 2008 relative à la Cour des comptes et aux chambres régionales des comptes

L'article L 2313-1 du CGCT[19] prévoit en outre que la présentation synthétique annexée au budget primitif et au compte administratif et le rapport d'orientations budgétaires sont mis en ligne sur le site internet de la collectivité territoriale - ou par tout autre moyen de publicité - au plus tard 15 jours après leur adoption par l'assemblée délibérante[20].

En second lieu, la loi NOTRe a créé un article L1611-9 du CGCT prescrivant à l'Exécutif d'une collectivité territoriale, en amont de toute opération exceptionnelle d'investissement, de présenter à l'assemblée délibérante une étude relative à l'impact pluriannuel de cette opération sur les dépenses de fonctionnement[21].

En troisième et dernier lieu, l'article 110 de la loi NOTRe crée une expérimentation de la certification des comptes publics locaux, afin de garantir que les comptes sont réguliers, sincères et qu'ils donnent une image fidèle du résultat de [la] gestion, de leur patrimoine et de leur situation financière.

La certification est une opinion écrite et motivée sur les comptes annuels d'une entité qu'un auditeur externe indépendant formule sous sa propre responsabilité.[22] ; le texte de la loi précise qu'elle porte sur « *la nature des états financiers, des normes comptables applicables, du déploiement du contrôle interne comptable et financier ou encore des systèmes d'information utilisés* ».

L'expérimentation est actuellement menée par 25 collectivités volontaires *de toutes natures et de toutes* tailles ; elle devrait arriver à son terme à la fin de l'année 2022 ; le gouvernement pourra alors tirer des enseignements des avancées obtenues comme des difficultés rencontrées pour étudier les modalités de son éventuelle extension, en prenant de surcroît modèle sur les pratiques observées dans l'Union européenne.

De fait, les premiers exercices de certification à blanc réalisés dans le courant de l'année 2021 ont montré l'ampleur de la tâche à réaliser et la majeure part des collectivités expérimentatrices se sont vu opposer en l'état une impossibilité de certifier.[23]

Les décisions prises à cet endroit ont quelques causes communes, notamment les incertitudes concernant les recettes, qu'il s'agisse des montants des dotations ou des recettes fiscales ; d'autres difficultés fréquemment rencontrées touchent le retard accumulé dans l'inventaire et la valorisation du patrimoine.

Plus généralement, beaucoup de collectivités paraissent insuffisamment avancées dans la construction d'une démarche de management des risques robuste et inclusive.

A cet égard, il apparaît que les collectivités ne peuvent se dispenser de déployer concurremment la cartographie des risques comptables et financiers d'une part et la cartographie des risques informatiques d'autre part, tant il apparaît que celles-ci sont en interaction constante.

[19] Cet article est issu de l'article 191 de la loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019

[20] L'article R 2313-8 du CGCT issu du décret n° 2016-834 du 23 juin 2016 précise les conditions dans lesquelles les documents budgétaires et financiers sont mis en ligne

[21] Ces dispositions sont issues du même article 107 de la loi NOTRe. Les seuils en pourcentage des recettes réelles de fonctionnement ou en valeur absolue ont été fixés par le décret n° 2016-892 du 30 juin 2016

[22] Cour des comptes. (2019). « Bilan intermédiaire de l'expérimentation de la certification des comptes locaux » https://blog.landot-avocats.net/wp-content/uploads/2019/06/20190619-rapport-bilan-experimentation-certification-comptes-locaux.pdf

[23] Voir notamment l'article de la Gazette des communes du 7 octobre 2021 « Une première certification à blanc des comptes en forme d'avertissement »

Le lien entre les risques comptables et financiers d'une part et les risques informatiques d'autre part résulte de l'étroite connexion qu'il y a entre l'efficience du Système d'information d'une collectivité et la fiabilité de son reporting, qui conditionne lui-même la qualité de son pilotage.

Cette observation souvent répétée est une incitation pour les collectivités à réaliser une cartographie des risques non pas segmentée et restreinte à certains aspects de leur fonctionnement mais au contraire d'emblée étendue à l'ensemble des fonctions supports concourant à la mise en œuvre des politiques dont elles ont la charge.

→ Voir **Fiche technique 4**

Expérimentation de la certification des comptes dans les collectivités locales (2017-2023)

L'impulsion donnée par la loi NOTRe a été continuée et renforcée

Ainsi le nouvel article L 243-9 du Code des juridictions financières issu de l'article 28 de l'ordonnance n° 2016-1360 du 13 octobre 2016, prévoit un renforcement de l'action des chambres régionales des comptes *via* l'obligation faite à l'exécutif de la collectivité territoriale de présenter un rapport sur les actions entreprises à la suite des observations formulées par les magistrats financiers dans un délai d'un an à compter de la présentation du rapport d'observations définitives à l'assemblée délibérante.

En outre l'article 143-9 du même code prévoit que le rapport public annuel de la Cour des comptes une présentation « *des suites données aux observations et recommandations de la Cour des comptes et des chambres régionales et territoriales des comptes, établie sur la base de comptes rendus que les destinataires de ces observations ont l'obligation de leur fournir* ».

De même, l'article 242 de la loi de finances pour l'année 2019[24] invite les collectivités territoriales et leurs groupements volontaires à mettre en place un Compte financier unique, à titre expérimental à compter de l'exercice budgétaire 2021 et pour une durée maximale de trois exercices budgétaires.

Proposé sous forme de recommandation par la Cour des comptes dans son premier rapport sur les finances publiques, en date du 14 octobre 2013, le Compte financier unique vise, par la fusion du compte administratif produit par l'ordonnateur et du compte de gestion établi par le comptable public, à simplifier et améliorer la qualité de l'information financière dans les collectivités territoriales[25].

Ce nouvel instrument a également pour objet d'enrichir les informations disponibles par l'ajout de la capacité d'autofinancement et de la capacité dynamique de désendettement et la présentation sur quatre ans de l'évolution des recettes et des dépenses [26].

Ces dispositions récentes contribuent à la mise en place d'un corps de recommandations normées et parfaitement traçables quant à leurs motifs et aux suites données ; chaque collectivité aura en outre tout loisir de les consolider sous la forme de guides de bonnes pratiques destinés à sécuriser et rationaliser la gestion de leurs différentes ressources.

[24] Loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019

[25] Dans un rapport remis en août 2017 à la demande du ministre chargé de l'économie et des finances, l'Inspection générale des Finances (IGF) et l'Inspection générale de l'Administration (IGA) ont esquissé la maquette du CFU, qui reprend des éléments aujourd'hui disséminés dans les deux documents de clôture : situation patrimoniale, information sur l'exécution du budget, annexes informatives et autres informations (dont les ratios financiers).

[26] Le Nocher, B. (2020). *Le paradoxe de la transparence financière dans les collectivités : Un enjeu ancien, une mise en œuvre récente.* https://www.lagazettedescommunes.com/690608/le-paradoxe-de-la-transparence-financiere-dans-les-collectivites-un-enjeu-ancien-une-mise-en-oeuvre-recente/?abo=1

En conséquence, on voit s'affirmer une forte dimension de pilotage et maîtrise des risques comptables et financiers associés à chaque exercice budgétaire ; cette tendance est une incitation forte à la mise en place de cartographies de risques progressivement étendues à l'ensemble des événements et interactions susceptibles de faire obstacle au bon fonctionnement des collectivités.

La dynamique ainsi créée prend appui sur une demande croissante d'exemplarité des collectivités territoriales dans la conduite de leurs politiques publiques et l'utilisation des deniers publics.

Si l'expérimentation de la certification des comptes publics locaux et du compte financier unique conduisent à des résultats probants, il est probable que les collectivités seront amenées à développer des méthodes de gestion propres à assurer une parfaite transparence vis-à-vis des tiers et à donner les assurances attendues en termes de maîtrise des principaux risques comptables et financiers.

Reporting extra-financier

Enfin, les collectivités de plus en plus largement amenées à rendre compte des progrès réalisés et des difficultés éventuellement rencontrées sur différents sujets transverses tels que l'égalité entre hommes et femmes, l'impact environnemental des politiques menées.

On retrouve en particulier cette préoccupation dans la directive 2014/95/UE du Parlement européen et du Conseil du 22 octobre 2014 relative à « *la publication d'informations non financières et d'informations relatives à la diversité par certaines grandes entreprises et certains groupes* ».

Le texte en question, entré en vigueur à compter du 1er janvier 2017, concerne seulement les acteurs privés ; il prévoit l'ajout d'une déclaration non-financière au rapport de gestion contenant toute information pertinente pour ses utilisateurs finaux.

« *Cette directive a pour objet l'intégration d'informations non financières pour une amélioration de la compréhension des incidences d'une activité sur la société. Les entreprises sujettes de la directive doivent « donner une image complète et fidèle de leurs politiques, de leurs résultats et de leurs risques » (directive 2014/95/UE, § 5). Les informations à fournir ont trait aux problématiques environnementales, sociales et de lutte contre la corruption.* »[27]

Toutefois, l'intégration de telles données pose le problème de leur degré de fiabilité.

« *Le processus d'assurance sur l'exactitude, la complétude et la disponibilité des données n'est pas clairement défini.* (…) *La nature de l'assurance et des vérifications conduites peut varier ; il n'existe encore aucune consigne universelle en matière d'assurance dans ce domaine et la majorité des rapports sont aujourd'hui publiés sans ou avec un faible niveau d'assurance externe.* »[28]

Cette problématique touche également les collectivités territoriales.

On la retrouve notamment dans les modalités de préparation et d'élaboration des rapports d'avancement de diverses études de synthèse et de prospective telles que les Schémas régionaux d'aménagement, de développement durable et d'égalité des territoires (SRADDET) et les Schémas régionaux du climat, de l'air et de l'énergie (SRCAE).

[27] Rapport d'étude Audencia « Quelles connexions entre la comptabilité financière et le non-financier *?* Développement durable et immatériel, état des lieux des représentations en comptabilité financière » - Section 1.2.2.2 - Juillet 2020

[28] Publication de l'IIA (Institute of internal auditors) Tone at the Top n° 75 (décembre 2015) - « Au-delà des chiffres : le nouveau monde du reporting non financier »

Pour résumer…

La mise en place d'une démarche assurantielle constitue une réponse pertinente aux incertitudes croissantes pesant sur l'environnement institutionnel, économique et social des collectivités locales.

Cette démarche s'inscrit également dans une évolution réglementaire qui pousse les décideurs territoriaux à une meilleure connaissance des menaces et opportunités associées à leur action afin de développer les outils décisionnels propres à faciliter des choix éclairés.

En outre, les collectivités sont appelées à prendre activement part à de nouvelles formes de coopération territoriale associant de multiples acteurs publics et privés ; or elles pourront affirmer et consolider le rôle moteur qui leur revient dans la seule mesure où elles apporteront concurremment les gages suffisants d'une bonne gestion inscrite dans la durée.

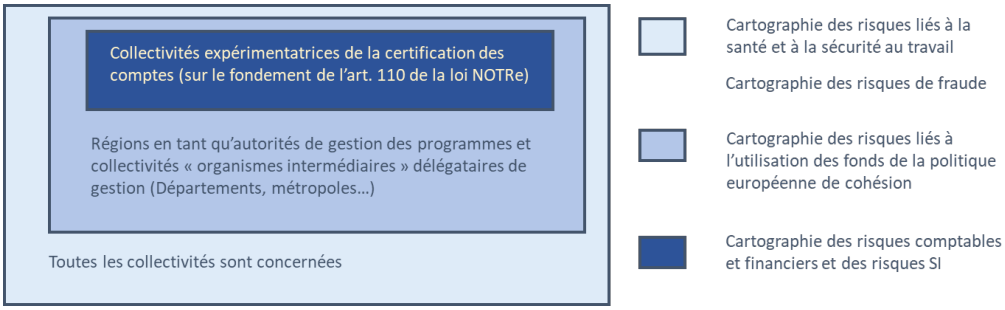
En conséquence, des obligations réglementaires aussi bien que des considérations d'opportunité peuvent pousser au déploiement d'un dispositif de connaissance et maîtrise des risques adapté aux besoins et enjeux de chaque territoire.

Des seuls éléments qui précèdent, il ressort que :

- l'ensemble des collectivités sont tenues d'une part de cartographier les risques liées à la sécurité et à la santé au travail et d'autre part de cartographier les risques d'atteinte à la probité et de mettre en œuvre des mesures de maîtrise proportionnées ;
- les collectivités investies de la responsabilité de gestion de crédits de la politique de cohésion européenne doivent établir la cartographie des risques associés à l'utilisation de ces financements et y donner les réponses appropriées ;
- les collectivités engagées dans une expérimentation de la certification des comptes sont généralement appelées à réaliser une revue complète de leurs risques comptables et financiers ainsi que des risques informatiques associés de manière à structurer leur contrôle interne et à réunir les conditions de leur auditabilité future.

Cette liste ne prétend pas à l'exhaustivité... On peut par exemple y ajouter la prévention du risque d'inondation désormais partagée entre l'État et les collectivités territoriales compétentes et d'autres domaines particuliers encore, généralement liés à la sécurité des personnes et des biens. Elle vise seulement à illustrer une tendance émergente forte ; chaque collectivité pourra mener des recherches complémentaires pour connaître les obligations réglementaires qui lui sont spécifiquement applicables.

<u>Quelles collectivités sont tenues de mettre en place une cartographie des risques ?</u>



1-B Donner une assurance raisonnable de l'atteinte de ces objectifs

L'atteinte des objectifs précédemment cités est soumise à des événements dont les conséquences sont potentiellement bénéfiques (aléa positif) ou préjudiciables (aléa négatif).

Ainsi et dès lors qu'elle a pu mesurer les objectifs qu'il lui appartient de réaliser dans le cadre d'une démarche assurantielle de moyen et long terme, une collectivité se doit d'identifier les freins susceptibles d'y être mis et à l'inverse les opportunités qui pourraient être exploitées pour faciliter ses desseins.

Ces obstacles potentiels à la réalisation des objectifs de la collectivité prennent la forme de risques.

Qu'est-ce qu'une démarche assurantielle ?

Une démarche assurantielle de contrôle et de management des risques a pour objet de donner aux instances dirigeantes d'une collectivité l'assurance raisonnable que les objectifs contenus dans le projet de mandat pourront être atteints dans les délais prévus et plus généralement que son fonctionnement répond aux critères d'une gestion efficiente et responsable.

Cette assurance raisonnable repose sur une revue complète des risques auxquels cette collectivité est exposée - compris tout de moins comme la possibilité de survenance d'événements défavorables - et la mise en œuvre de mesures de maîtrise propres à réduire la probabilité et/ou l'impact des risques les plus critiques.

Le niveau de maîtrise des risques est évalué à chaque échelon de la chaîne de traitement par une fonction de contrôle interne et en dernier ressort par le responsable de l'audit interne, sous la supervision éventuelle d'auditeurs externes et/ou de régulateurs habilités.

Quels risques sont à prendre en compte au titre de cette démarche ?

Les risques sont généralement perçus comme des entraves à l'atteinte d'un résultat désirable ; ils peuvent toutefois être utilisés comme des leviers d'action au service d'une stratégie globale de conformité et de qualité[29].

A cet égard, il paraît pertinent de retenir la définition neutre donnée par le Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP) :

« *Possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité*. »

Cette définition peut être mise en regard de celle donnée par la norme ISO 31000-2018 relative au management du risque, laquelle décrit le risque comme « l'effet de l'incertitude sur les objectifs » ; en complément, l'ambivalence de la notion d'effet est ainsi rappelée : « *Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois et traiter, créer ou entrainer des opportunités et des menaces.* »

[29] Voir ci-après Section 2-A-2 - page 56

Dans cette continuité, la norme ISO 31000-2018 définit le management des risques comme un ensemble « *d'activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque* »[30]

Le management des risques se présente ainsi comme une part intégrante de la mise en œuvre de la stratégie de toute organisation, qu'elle soit publique ou privée.

Tous les risques sont à prendre en compte, qu'ils soient opérationnels, juridiques, stratégiques, managériaux, liés à la réputation, systémiques etc. en intégrant dans l'analyse à la fois des facteurs endogènes et exogènes.

Comment traiter ces risques ?

Selon la norme ISO 31000 relative au management des risques[31], tout risque doit être traité de l'une ou l'autre des manières suivantes :

- refus du risque : l'activité porteuse de risque est abandonnée (souvent difficile pour une collectivité dans un contexte de mission de service public) ;
- prise de risques : le risque est pris car les gains espérés sont supérieurs aux menaces encourues ;
- réduction de la probabilité de survenance ou de la gravité des impacts en cas de survenance ;
- partage du risque : transfert vers un assureur ou un tiers (Délégation de service public…).

Deux éléments sont à prendre en compte selon la norme pour procéder à ce choix :

- la balance entre les bénéfices et menaces associés à la prise du risque ;
- la comparaison entre les coûts engendrés par le traitement du risque et les coûts engendrés par la survenance dudit risque.

Sur ce dernier point, la mise en place d'une solution de traitement peut éventuellement produire des inconvénients, voire améliorer la situation d'un risque mais empirer la criticité d'un autre.

La phase de traitement s'inscrit dans une logique itérative, la mise en œuvre de plans d'actions efficaces modifiant le niveau de maîtrise des risques.

En conséquence, une collectivité engagée dans une démarche de management des risques se trouve dans la nécessité de réactualiser régulièrement les analyses déjà menées, et le cas échéant de mener à bien de nouveaux plans d'actions pour réduire les risques résiduels.

Une fois analysés, ces risques doivent être comparés afin de définir une stratégie de traitement en fonction du niveau d'appétence de la collectivité, qui doit être compris comme le degré de risque assumé pour atteindre les principaux objectifs qu'elle s'est fixés [32].

Ce dispositif doit contribuer à la création de valeur, à l'aide à la décision, à la détection des opportunités et ne surtout pas aboutir à « *un immobilisme annihilant toute action* »[33]. Il se doit de contribuer également à la préservation de cette valeur, en s'interrogeant sur la vulnérabilité de la collectivité face à des menaces de toute nature.

[30] Article 3 de la norme NF ISO 31000 :2018

[31] Voir Point 6-5 de la Norme

[32] Voir plus bas, Section 2-A-2

[33] Management du risque : une approche stratégique ; Géraldine Sutra ; Afnor éditions

1-B-1 Eléments de méthodologie

La méthodologie pour le déploiement d'une démarche assurantielle étendue à l'ensemble du fonctionnement de la collectivité et à la mise en œuvre des politiques dont elle a la charge puise principalement dans deux sources :

- la Norme ISO 31000-2018 relative au management du risque ;
- le dispositif des trois lignes de maîtrise des risques proposé comme la norme standard des travaux d'audit par l'IIA (*Institute of Internal Auditors*).

La norme ISO 31000-2018 envisage d'abord le management des risques comme une source de création et de préservation de la valeur ; les principes et les lignes directrices qu'elle fournit ne visent pas à la promotion d'une pratique uniforme, leur objet est plutôt d'harmoniser une accumulation empirique d'approches, de standards et de méthodes existants.

Dans son prolongement, le modèle des trois lignes de maîtrise des risques, à la fois proactif et défensif, a pour objet de faciliter la maîtrise des risques et des opportunités à l'échelle d'une organisation en proposant une grille de lecture commune pour évaluer les progrès réalisés dans ce sens et identifier les points de fragilité persistants.

En toute hypothèse, le point d'entrée est d'aligner les objectifs de la collectivité, sa politique de management des risques et ses obligations légales et responsabilités contractuelles ; le cadre du management des risques doit être intégré dans les processus de décisions et d'organisation de toutes ses activités, en veillant aux contextes internes et externes, aux responsabilités des différentes parties engagées et aux ressources disponibles au niveau stratégique et opérationnel.

Par ailleurs, la crise sanitaire de 2020 n'a pas été sans conséquence sur l'appréhension du management des risques et la prise en compte de ces thématiques dans les priorités stratégiques des nouveaux mandats.

La possibilité de survenance d'autres événements subits et aussi fortement disruptifs a pu donner à de nombreuses collectivités matière à réflexion pour construire et actualiser des Plans de continuité d'activité (PCA) propres à garantir la délivrance des services essentiels en toutes circonstances et à prévenir toute atteinte grave à leur fonctionnement ou à leur organisation interne.

Ces réflexions conduisent à rechercher des méthodes de détection et de protection des fonctions cruciales des collectivités qui reprennent les principes issus de la Norme ISO 31000-2018 et les renforcent dans le sens de l'acquisition de capacités spécifiques à la gestion de crise.

La création d'un Système de management de la continuité d'activité en temps de crise est un exercice complexe qui mobilise l'ensemble des parties engagées dans le fonctionnement de la collectivité et demande à être régulièrement testé, amélioré et actualisé.

Les prérequis et les éléments de méthode nécessaires à la bonne fin d'une telle démarche sont énoncés dans la Norme ISO 22301-2019 relative à la Sécurité et à la résilience des organisations confrontées à des risques majeurs.

→ Voir **Fiche technique 5**

Mode opératoire pour la mise en place d'un système de management de la continuité d'activité

Les principes directeurs

Conformément aux dispositions de la norme ISO 31000 de management du risque, toute collectivité engagée dans une démarche de construction méthodologique et opérationnelle engageant son fonctionnement sur le long terme doit appliquer huit principes directeurs.

Ces principes caractérisent le processus à conduire pour aboutir à une organisation parfaitement efficiente et évolutive.

Principes de management du risque

Source : Norme ISO 31000-2018
« Management du risque » (Fig 2)

Caractérisation du processus	Descriptif
Intégré	Le management des risques doit être appliqué à toutes les activités et métiers de la collectivité, quelle que soit la nature du processus auquel ils sont rattachés. En outre, le périmètre de l'exercice doit s'étendre aux organismes associés ainsi qu'aux organismes subventionnés.
Structuré et global	Il permet l'obtention de résultats cohérents, présentables et comparables
Adapté	Il prend en compte le contexte interne et externe de la collectivité et ses spécificités et le proportionne à sa taille et à ses enjeux
Inclusif	Il intègre toutes les parties prenantes dans la démarche.
Dynamique	Il permet la détection et la prise en compte de nouveaux risques tout en étant suffisamment souple pour modifier voire supprimer des risques obsolètes
Meilleure information disponible	Les données utilisées sont fondées sur des informations historisées et continuellement actualisées ainsi que sur les attentes futures. Il est tenu compte de l'ensemble des limites et incertitudes associées aux éléments collectés.
Facteurs humains et culturels	Le comportement humain et la culture influent sensiblement la conduite de la démarche, à tout niveau de responsabilité et à chaque étape.
Amélioration continue	Le management du risque tire les enseignements de l'expérience et y puise de la matière pour s'améliorer en continu.

Sur le fondement des huit principes précédemment énoncés, le management des risques se caractérise par un cadre organisationnel ayant vocation à permettre à la collectivité de structurer son fonctionnement et de le positionner au cœur de la gouvernance.

L'animation du management des risques dépend de l'état de maturité et de déploiement du dispositif, qui doit être évalué au commencement de toute démarche de structuration organisationnelle et fonctionnelle [34].

La norme ISO 31000 de management du risque inscrit ce cadre organisationnel dans une logique de cycle de cinq étapes pour lesquelles le leadership et l'engagement du dirigeant de la collectivité sont indispensables.

Les cinq étapes du cadre organisationnel de management des risques

Source : Norme ISO 31000-2018 « Management du risque » (Fig 3)

L'instance dirigeante de la collectivité porte la responsabilité de déterminer l'orientation stratégique et de créer l'environnement et les structures pour que la gestion des risques s'effectue efficacement.

Véritables sponsors de la démarche, l'Exécutif, la Direction générale et les éventuels organes de surveillance doivent démontrer régulièrement leur implication dans le dispositif de management du risque.

Leur intérêt se doit d'être régulier sur les avancées de la démarche et sur les résultats obtenus.

Plus généralement, il y a lieu d'attirer l'attention des contributeurs sur l'importance de leur engagement et sur la nécessité d'une disponibilité régulière pour contribuer aux analyses et à la mise en œuvre graduelle du dispositif.

[34] Voir ci-après Section 2-A

Les cinq phases de déploiement d'un dispositif de management des risques

	Phases	Contenu
1	**Intégration**	Le dispositif concerne l'ensemble des collaborateurs de la collectivité. Il couvre les risques liés aux organismes associés et aux organismes subventionnés. La norme rappelle le caractère dynamique et itératif du dispositif. Le cadre organisationnel s'inscrit dans une boucle conduisant à réaliser chaque étape et à s'assurer de son opérationnalité. Les éléments de contexte n'étant pas figés, cette boucle est en perpétuel recommencement. Le management des risques évolue dans le temps et ne se limite pas au seul exercice de cartographie.
2	**Conception**	Cette phase comprend : ▪ la compréhension du contexte interne et externe de la collectivité ; ▪ la définition de l'engagement en matière de management des risques ; ▪ l'attribution des rôles, des pouvoirs et des responsabilités. L'option retenue par la direction générale pour animer le dispositif sera déterminante lors de cette étape de désignation. Elle impactera le niveau d'implication attendue des propriétaires de risques, le recours éventuel à des correspondants dans les directions, etc. ; ▪ L'affectation des ressources nécessaires (humaines, techniques et documentaires) ; ▪ L'établissement d'une politique de communication et de concertation qui permettra de soutenir le cadre organisationnel.
3	**Mise en œuvre**	Le déploiement de ce cadre organisationnel doit s'inscrire dans une logique de projet. Par ailleurs, le manager des risques doit être positionné de manière à disposer de la transversalité nécessaire à la conduite de sa mission. Cette cohérence se traduira notamment par la compatibilité des calendriers entre les cycles de la collectivité et la dynamique du management des risques.
4	**Evaluation**	Afin de s'assurer que la trajectoire prise par le dispositif réponde bien aux objectifs fixés, il est nécessaire d'évaluer le dispositif mis en œuvre. Cette prise de recul et de hauteur permettra de s'assurer de l'efficacité de l'existant et de relever d'éventuels écarts, et d'apprécier les contributions réelles du dispositif à l'atteinte des objectifs stratégiques de la collectivité.
5	**Amélioration**	L'identification des forces et des faiblesses du dispositif s'inscrit dans une logique d'amélioration continue. Elle se traduira par des plans d'action permettant d'améliorer l'existant.

La combinaison des principes directeurs de la démarche et des étapes de déploiement susmentionnés permet de définir les principales étapes opérationnelles d'un processus de management du risque piloté par la gouvernance et à l'échelle de la collectivité.

Bien entendu, ce schéma global doit être adapté à chaque situation particulière mais il fournit un fil conducteur utile pour préparer et exécuter un projet aussi structurant pour les équipes et le territoire.

→ Voir **Fiche technique 6**

Le processus de management du risque

Les trois lignes de maîtrise des risques

La mise en place d'une fonction de responsable du contrôle interne s'est accompagnée de la formalisation d'un modèle de gouvernance fondé sur l'interaction de trois lignes distinctes de maîtrise des risques.

Une première prise de position de l'IIA (*Institute of internal auditors*) de janvier 2013[35] relayée par une communication jointe de l'Institut français de l'audit et du contrôle internes (IFACI) et l'Association pour le management des risques et des assurances de l'entreprise (AMRAE) en a fixé les bases tout en invitant à une application adaptée à chaque contexte.

Ce modèle fait notamment écho aux principes 7 et 10 du COSO 2013 relatifs respectivement à l'identification des risques associés à la réalisation des objectifs de l'organisation et au déploiement des activités de contrôle propres à maintenir ces risques à des niveaux acceptables.

Ses composantes sont ainsi réparties :

- la première ligne de maîtrise centrée sur un rôle opérationnel de management met en œuvre les vérifications au fil de l'eau contribuant à la maîtrise des risques;
- la deuxième ligne de maîtrise centrée sur un rôle d'expertise concourt à la mise en place d'un dispositif complet et interactif de management des risques ;
- la troisième ligne de maîtrise est celle de l'assurance fournie par l'audit interne.

Dans un tel schéma, le contrôle interne est une fonction partagée entre la première et la deuxième ligne de maîtrise ; de même et plus généralement la première et la deuxième ligne de maîtrise peuvent fonctionner de concert, à la différence de la troisième ligne qui doit demeurer indépendante[36].

La mise en place de trois lignes de maîtrise des risques constitue une assurance que se donne la collectivité face au risque d'être durablement affectée par la survenance d'un ou plusieurs des événements contraires auxquels elle se trouve exposée.

Dans une formulation plus positive, la combinaison des contrôles et vérifications indépendamment opérés à chacun des trois échelons du dispositif de maîtrise des risques permet de donner à la Direction générale et à l'Exécutif une assurance raisonnable quant à la bonne gestion de la collectivité et à l'atteinte des objectifs du projet de mandat.

[35] Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces - 2013. Ce premier position paper a été actualisé en 2020.

[36] A la réserve des modalités de coopération possibles entre la deuxième ligne et la troisième ligne pour la mise en place de la méthodologie du management des risques - voir Fiche technique n° 15

Le cadre de répartition des travaux liés à la gestion des risques et au contrôle de leur degré de maîtrise repose sur une forte coopération entre plusieurs entités de la collectivité fonctionnellement non dépendantes les unes des autres, de manière à écarter toute possibilité de pression sur les personnes et afin d'éliminer tout élément propre à atténuer l'objectivité de leurs conclusions respectives.

Toutefois, la simple désignation de ces différentes fonctions ne suffit pas, il faut encore décrire leurs interactions et fixer des règles communes de validation et d'exploitation des données collectées.

En effet, l'absence d'approche cohérente et coordonnée peut conduire à une utilisation inefficace des ressources limitées à la gestion des risques et au contrôle, ainsi qu'à une situation où les risques significatifs ne seraient pas identifiés ou mal gérés.

La distribution des rôles et responsabilités entre chacun des échelons de maîtrise fournit un moyen simple et efficace pour améliorer la communication en matière de gestion des risques et de contrôle, en clarifiant le positionnement des différents acteurs.

Ainsi, il y a lieu de distinguer trois groupes de fonctions impliquées dans la gestion efficace des risques :

- les fonctions qui endossent et gèrent les risques ; elles ont également la responsabilité de la mise en œuvre des mesures correctives permettant de remédier aux déficiences des processus et des contrôles ;
- celles qui assurent le suivi des risques ; il s'agit des fonctions de gestion des risques, de contrôle interne et de conformité chargées de contribuer à la mise au point et/ou à la surveillance des contrôles relevant de la première ligne de maîtrise ;
- enfin celles qui fournissent une assurance indépendante sur l'efficacité de la gouvernance, de la gestion des risques et du contrôle interne.

→ Voir **Fiche technique 7**

Les trois lignes de maîtrise des risques

1-B-2 Les acteurs

La conduite d'une démarche assurantielle globale repose sur une pluralité d'acteurs suivant une feuille de route précisément élaborée dès avant le démarrage du projet.

Son pilotage échoit ainsi tout naturellement à la gouvernance de la collectivité composée de la direction générale et de l'exécutif, avec l'appui éventuel de personnalités extérieures qualifiées.

Sa mise en œuvre opérationnelle revient aux fonctions ayant part aux trois lignes de maîtrise des risques articulées autour de la fonction du contrôle interne.

Il s'agit du cœur du dispositif où se concentreront l'essentiel des travaux et des missions ; la gouvernance s'assure de son efficacité et de sa pertinence quelle que soit l'évolution des risques de la collectivité.

Enfin, un rôle de conseil et d'expertise peut être dévolu à des fonctions associées, pour autant que de besoin.

Acteurs en charge de la gouvernance

Bien que situés en dehors des trois lignes de maîtrise, les organes de gouvernance ont une responsabilité essentielle dans la gestion globale des risques.

Ils sont collectivement tenus de rendre compte de la définition des objectifs de la collectivité et des stratégies à adopter pour les atteindre.

En référence à l'article 5.2 de la Norme ISO 31000-2018, les acteurs en charge de la gouvernance ont notamment la charge :

- de veiller au correct alignement du management des risques avec la stratégie de la collectivité et les objectifs qui en découlent d'une part et avec la culture de la structure d'autre part ;
- de garantir le bon niveau des ressources allouées ;
- de communiquer aux parties prenantes l'ensemble des informations dont ils ont besoin de connaître sans rien en retrancher ou diminuer ;
- d'établir des niveaux et des types de risque pouvant être pris par la collectivité ;
- de promouvoir un suivi systématique des actions engagées.

A cet égard, ils s'assurent de la mise en place d'un environnement favorable à la mise en œuvre d'une démarche assurantielle globale et prennent les arbitrages requis quant à l'appétence de la collectivité au risque, comme cela est présenté à la section 2-A ci-après.

Ainsi deux profils sont principalement engagés dans la gouvernance de la démarche :

- la Direction générale de la collectivité;
- l'échelon décisionnaire politique qui peut être le maire ou le président de la collectivité, un membre de l'exécutif désigné pour le représenter ou même d'une commission permanente dédiée composée d'élus issus des divers groupes siégeant dans l'assemblée.

Le cas échéant, ces acteurs peuvent prendre appui sur une instance de pilotage créée *ad hoc* pour apporter son expertise et donner des avis techniques - voir la Section 1-B-3 ci-après.

Un plein engagement de la gouvernance est une condition nécessaire du succès de la démarche.

En gage de sa solidité, cet engagement doit reposer sur une vision stratégique de moyen et long terme : « *La gouvernance d'une collectivité a la responsabilité de mettre en œuvre le budget, les projets et les orientations approuvées par le conseil. Les risques sont indissociables du projet de mandat. Cette surveillance par la gouvernance suppose de déterminer les enjeux clés qui devront faire l'objet d'une vigilance spécifique et les modalités d'exercice de cette surveillance en distinguant ce qui relève des différents acteurs.* »[37]

→ Voir **Fiche technique 8**

Profils engagés dans une démarche de management des risques - Acteurs en charge de la Gouvernance

[37] Maîtrise des risques dans les collectivités territoriales - Fiche relative au Principe n° 1 du cadre de référence du COSO-ERM 2017 (« Assurer une surveillance des risques par la gouvernance ») - Publication conjointe CIAT-IFACI - 2019

Les acteurs en charge des trois lignes de maîtrise des risques forment le cœur opérationnel du dispositif assurantiel établi à l'échelle de la collectivité.

On trouve parmi eux les fonctions clés requises pour le lancement et la conduite de la démarche :

- le manager des risques qui a un rôle d'assemblier et de coordonnateur du projet sur l'ensemble de ses étapes ;
- les directions métiers en charge de la gestion au jour le jour des risques identifiés et dites à ce titre « propriétaires » de ces risques ;
- le responsable de la fonction de contrôle interne et le responsable de l'audit interne ont la charge de l'évaluation du niveau de maîtrise des risques à leurs niveaux d'intervention respectifs.

Chacun de ces acteurs a une part essentielle dans l'architecture d'ensemble.

Par ailleurs, le manager des risques est l'interlocuteur tout indiqué de la gouvernance ; il lui revient de présenter les progrès réalisés et les difficultés éventuellement rencontrées. De même c'est à lui de rechercher les arbitrages nécessaires à l'avancement du chantier et de rendre compte de leur bonne exécution.

Possibilité d'une approche progressive et graduelle de la maîtrise des risques

Les dernières enquêtes nationales réalisées montrent que peu de collectivités se sont dotées d'un dispositif de contrôle interne et qu'une plus faible proportion d'entre elles encore ont mis en place une fonction d'audit interne[38].

Dans une collectivité donnée, l'absence de ressources dédiées à ces travaux ne constitue toutefois pas un obstacle infranchissable au déploiement d'une démarche efficace de maîtrise des risques.

La chaîne d'évaluation peut en effet se borner à la première ligne de maîtrise et à un manager des risques positionné sur la seconde ligne sans pour autant cesser de produire des données exploitables pour un pilotage assurantiel de la collectivité.

Dans ce cas, il est de la responsabilité de l'encadrement de formaliser les procédures et traitements à la charge des services opérationnels puis d'en vérifier la correcte application dans le cadre de leurs fonctions de supervision et de surcontrôle.

Une collectivité qui aurait fait ce choix pourra ultérieurement renforcer sa seconde ligne de maîtrise des risques en y adjoignant un responsable de la fonction de contrôle interne nommément désigné.

De même, une collectivité dépourvue de la troisième ligne de maîtrise serait tout à fait fondée à la créer par étape plutôt que d'un bloc ; à cet effet, elle peut d'abord sous-traiter ses travaux d'audit puis éventuellement créer la fonction en interne de manière à étendre la chaine de validation et renforcer ainsi le degré de confiance susceptible d'être accordé aux outils et méthodes utilisés.

[38] Voir les chiffres donnés dans l'Introduction

Ainsi et sous la réserve d'une approche graduelle, toute collectivité engagée dans une démarche assurantielle globale sera amenée à pourvoir les trois lignes de maîtrise de la manière suivante.

Ligne de maîtrise du risque	Agents concernés
Première ligne	La première ligne de maîtrise correspond au management des risques de la collectivité, tel qu'il est réalisé dans son fonctionnement au fil de l'eau. Cette mission incombe principalement aux directions métier en charge des processus auxquels sont rattachés les différents risques identifiés [39]. Chacune de ces directions dispose d'un portefeuille de risques plus ou moins étendu dont elle doit assurer la maîtrise au moyen de mesures préventives et/ou correctrices prédéterminées. Les tâches correspondantes sont du ressort des agents opérationnels prenant part à la chaîne de traitement, sous la supervision de leur management de proximité. Pour une part de ses missions, le responsable de la fonction de contrôle interne peut prendre directement part à ces travaux et contribuer ainsi au renforcement du système de maîtrise.
Deuxième ligne	La deuxième ligne de maîtrise recouvre une fonction d'expertise complémentaire qui est principalement dévolue au manager des risques. Le manager des risques veille à la mise en place d'une cartographie des risques couvrant les différents volets du fonctionnement de la collectivité ; il vérifie que leur criticité est correctement évaluée et ceci à échéance régulière. Pour l'autre part de ses missions, le responsable de la fonction de contrôle interne est également amené à intervenir sur la seconde ligne de maîtrise. Dans ce cadre, il supervise les vérifications à la charge des directions métier et apporte tous les éléments de méthodologie utiles. On y trouve également le Responsable qualité ainsi que les différents agents en charge de la compliance (hygiène, santé et sécurité au travail, protection des données à caractère individuel…) dans la mesure où leurs travaux concourent au management des risques.
Troisième ligne	La troisième ligne de maîtrise des risques correspond aux fonctions d'audit interne. Un Responsable de l'audit interne est en charge de cette fonction. Il teste l'efficience et la robustesse des procédures de management des risques existantes ; dans ce cadre, il identifie d'éventuelles insuffisances, émet des recommandations visant à les corriger et s'assure de leur correcte mise en œuvre.

[39] Les directions métiers sont également dits « propriétaires » de ces risques

Ces différents acteurs interviennent successivement pour établir, éprouver et éventuellement ajuster le niveau de maîtrise de chacun des risques identifiés.

Les agents positionnés à chacun de ces échelons ont la possibilité de tester la robustesse et l'efficience du dispositif de contrôle établi au titre de la maîtrise du risque et de mettre en question la note attribuée[40] s'ils relèvent des dysfonctionnements et/ou des défauts de conception propres à en compromettre l'efficacité.

A leur niveau respectif, ils contribuent à la consolidation et à l'extension de la cartographie des risques jusqu'à en faire un outil essentiel de référence et de partage à l'échelle de la collectivité et des différentes parties engagées.

En outre, différentes instances peuvent intervenir dans le processus d'évaluation du dispositif de maîtrise des risques en tant que régulateurs ou auditeurs externes.

A titre d'exemples, on peut ainsi citer :

- les contrôles de la Chambre régionale des comptes portant sur la régularité des comptes et les performances de gestion ;
- les investigations menées par la Commission interministérielle de coordination des contrôles, les services d'audit de la Commission européenne ou la Cour des comptes européenne au titre de la mise en œuvre des financements de la politique européenne de cohésion ;
- les contrôles de l'Agence française anti-corruption (AFA) ;
- les audits de conformité de la Commission nationale de l'informatique et des libertés pour le traitement des données à caractère personnel[41].

Dans leurs attributions respectives, ces autorités sont appelées à statuer sur la qualité du fonctionnement de la collectivité et à émettre, sur ce fondement, une opinion susceptible d'affecter la note de maîtrise de tout ou partie des risques couverts.

Leur appréciation du niveau de maîtrise du risque prévaut sur l'opinion de l'ensemble des niveaux de contrôle et d'audit internes à la collectivité.

Il appartient à chaque collectivité d'organiser et formaliser un dispositif de maîtrise des risques proportionné à ses possibilités et à l'enjeu associé à la réussite de cet exercice.

Dans tous les cas, elle dispose d'une première ligne de maîtrise constitué des agents opérationnels en charge des tâches considérées et de leur encadrement.

La mise en place de lignes de maîtrise additionnelles permet d'attester la fiabilité des mesures existantes de surveillance et de réduction des risques au moyen d'avis croisés et indépendants ; elle peut fortement contribuer à l'instauration d'un partenariat de confiance entre la collectivité et tout ou partie des auditeurs et régulateurs externes présents dans son environnement large.

→ Voir **Fiche technique 9**

Profils engagés dans une démarche de management des risques - Acteurs en charge des trois lignes de maîtrise

[40] Voir Fiche technique n° 13

[41] Ces audits sont conduits sur le fondement de l'article 58 1-b du Règlement général sur la protection des données n° 2016/679 du 27 avril 2016

La philosophie et les modalités d'utilisation du modèle des trois lignes de maîtrise des risques sont déterminées dans des prises de position - ou Position papers - successivement publiés par l'IIA (Institute of internal auditors) après consultation de l'ensemble des parties engagées.

En premier lieu, un position paper de 2013[42] a fixé les principales caractéristiques de ce dispositif assurantiel global, susceptible d'être adapté à toute organisation privée ou publique.

Ces éléments ont cependant été de nouveau examinés à la lumière des évolutions rapides d'un monde toujours plus interconnecté et exposé à des menaces et opportunités croissantes.

La tendance ainsi observée invite à la mise en place d'organisations plus souples, plus résilientes et plus aisément modulables selon les circonstances rencontrées.

Ainsi, un nouveau position paper de 2020[43] rend compte de cette réflexion.

Ce document est constitué de plusieurs principes constitutifs d'une doctrine globale et cohérente, propre réunir les conditions d'un large consensus.

Parmi ceux-ci, le principe n° 3 reprécise les rôles et responsabilités des première et seconde ligne de maîtrise sur les bases suivantes :

« *Les rôles de la première ligne sont plus directement liés à la fourniture de produits et/ou services aux clients de l'organisation et incluent les fonctions supports. La deuxième ligne recouvre quant à elle des activités d'appui à la gestion des risques.* »

L'approche retenue a pour effet de faire remonter l'ensemble des fonctions support dans la première ligne, comme cela est clairement rappelé :

« *Certains considèrent les fonctions support (services RH, administratifs, généraux, etc.) comme des rôles de deuxième ligne. Dans le Modèle des Trois Lignes, les rôles de première ligne englobent à la fois les activités « front of house » et « back office », tandis que les rôles de deuxième ligne intègrent les activités complémentaires axées sur les risques.* »

De même, il est désormais convenu que le terme « lignes » ne désigne pas des éléments structurels particuliers d'une organisation mais différents rôles que de mêmes acteurs du modèle peuvent exercer simultanément.

Ces éléments sont synthétisés dans la suite de la proposition :

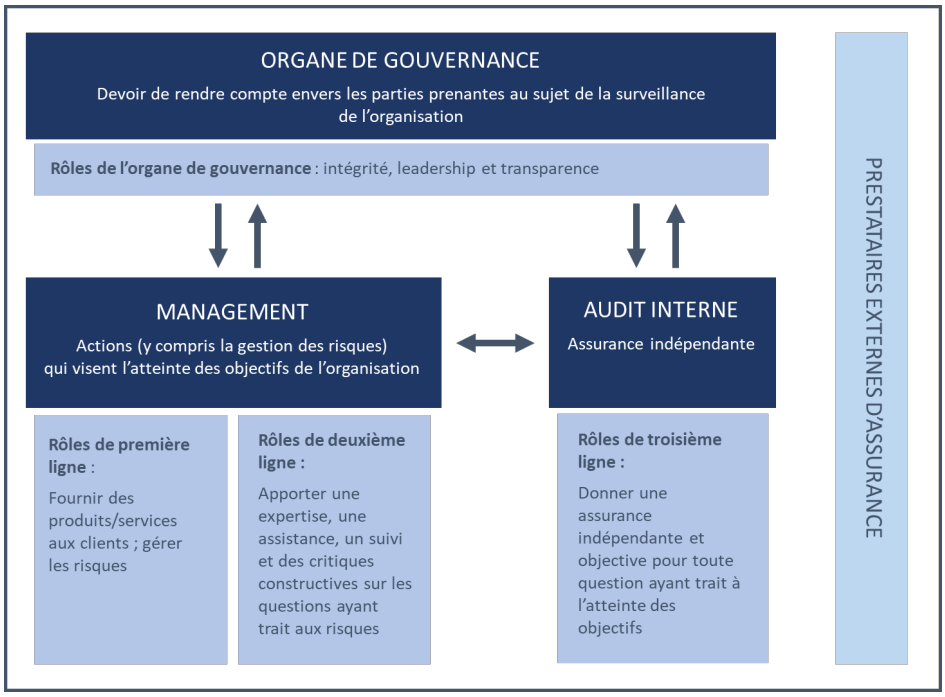
« *Les première et deuxième ligne peuvent être fusionnées ou séparées. Certains rôles de deuxième ligne peuvent être confiés à des spécialistes chargés d'apporter une expertise complémentaire, une assistance, un suivi et des critiques constructives aux acteurs de la première ligne. D'autres peuvent être orientés sur des objectifs précis dans le domaine de la gestion des risques - conformité aux lois et règlements et comportement éthique acceptable, contrôle interne, sécurité des systèmes d'information, développement durable, assurance qualité, etc. -, et même se voir confier de plus grandes responsabilités en la matière, comme le management des risques de l'entreprise (ERM).*»

Cependant, la gestion des risques est d'abord assurée au niveau de la deuxième ligne de maîtrise tandis que la première ligne est concentrée sur leur identification et leur traitement au quotidien.

[42] Prise de position de l'IIA - Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficace - Janvier 2013

[43] Le modèle des trois lignes de maîtrise de l'IIA - Version 2020 des trois lignes de maîtrise

Modèle des trois lignes de maîtrise - Position paper IIA de 2020



Le Management est au cœur du dispositif dans la mesure où il couvre la première et la seconde ligne de maîtrise ; il conduit ces missions dans un dialogue permanent avec la gouvernance et l'audit interne.

Ses responsabilités sont ainsi décrites.

« *Rôles de la première ligne :*

- *Oriente et conduit les actions (y compris de gestion des risques) et exploite les ressources à disposition pour réaliser les objectifs de l'organisation.*
- *Entretient un dialogue permanent avec l'organe de gouvernance et lui rend compte i) des résultats budgétés, prévisionnels et réalisés au regard des objectifs de l'organisation, et ii) des risques.*
- *Met en place et préserve des structures et des processus adéquats pour la gestion des opérations et des risques (contrôle interne y compris).*
- *Veille au respect des exigences d'ordre juridique, réglementaire et éthique.*

Rôles de la deuxième ligne :

- *Apporte une expertise complémentaire, une assistance, un suivi et des critiques constructives en matière de gestion des risques, notamment sur les aspects suivants :*
    - *le développement, la mise en œuvre et l'amélioration continue des pratiques de gestion des risques (contrôle interne y compris) au niveau d'un processus, d'un système ou d'une entité ;*
    - *la réalisation des objectifs de gestion des risques : conformité aux lois et règlements et comportement éthique acceptable, contrôle interne, sécurité des systèmes d'information, développement durable, assurance qualité, etc.*
- *Produit des analyses et des rapports sur l'adéquation et l'efficacité de la gestion des risques (contrôle interne y compris).* »

Zoom sur deux acteurs clés du dispositif

La cartographie des risques est un outil essentiel et déterminant pour le manager des risques et le responsable de la fonction de contrôle interne.

Dans une collectivité où les deux missions seraient existantes, ces deux acteurs contribuent à son élaboration et à son actualisation.

L'un et l'autre interviennent principalement sur les risques non maîtrisés ou mal maîtrisés dont la criticité est élevée.

Sur ce champ commun, ils exerceront un rôle différent dans le traitement des risques ; la détermination précise de leurs périmètres d'intervention respectifs est donc nécessaire pour écarter toute possibilité de chevauchement ou redondance.

Pour le **responsable de la fonction de contrôle interne**, la cartographie des risques est un état des lieux des risques à date.

Elle va lui permettre d'identifier les risques non maîtrisés ou mal maîtrisés pour lesquels des contrôles complémentaires devront être appliqués.

Connaître les risques lui permettra de sécuriser les processus afin d'éviter qu'ils ne se produisent ou d'en limiter les impacts.

Acteur clé de l'identification des risques et en contact permanent avec les services opérationnels, il identifie les dispositifs de maîtrise en place, mesure leur efficacité et propose tout plan d'action propre à corriger les fragilités éventuellement constatées.

Le **manager des risques** a une intervention plus globale sur les risques en accompagnant les managers dans le choix du traitement des risques (acceptation, assurance, traitement…).

Animateur du dispositif de maîtrise des risques, il identifie les failles/menaces qui pèsent sur les objectifs de la collectivité et du projet politique.

Il analyse les incidents qui se sont produits ou qui pourraient se produire afin de proposer des actions afin de les éviter.

Sachant que tous les risques ne peuvent être évités, il intervient également dans la gestion des crises en élaborant un plan et en conseillant la direction générale sur les dispositifs nécessaires à mettre en place.

La cartographie des risques lui permettra donc d'identifier les risques, de les hiérarchiser et de prioriser les actions à mettre en œuvre.

Il n'y a pas vraiment de schéma type en termes d'organisation.

A la question « vaut-il mieux recruter un contrôleur interne ou un manager des risques ? » on n'apportera pas de réponse définitive, claire et tranchée.

Leurs missions sont complémentaires et évoluent en parallèle : le management des risques et le contrôle interne sécurisent les processus de la collectivité afin de l'accompagner dans la réalisation de ses objectifs et de l'aider à tenir ses engagements. Ils interviennent tous les deux sur les dérives soit de manière préventive, soit de manière curative.

De ce fait, ils contribuent tous les deux pleinement au pilotage de la collectivité.

Pour conclure, la collectivité s'adaptera souvent en fonction des compétences présentes en interne ou du type de recrutement qu'elle pourra réaliser. Dans tous les cas, si plusieurs personnes travaillent sur le management des risques et/ou le contrôle interne, il conviendra de travailler en bonne harmonie, de définir un vocabulaire commun et de communiquer régulièrement sur les travaux que chacun mène. Il semble également indispensable d'établir un RACI (*Responsibility assignment matrix*) afin de définir et de s'accorder sur le rôle de chacun.

Dès avant la mise en place de la cartographie, le manager des risques a tout intérêt à prendre l'avis de collègues disposant d'une technicité particulière dans les domaines reconnus comme les plus exposés et plus encore sur les questions soumises à une obligation réglementaire comme la lutte anti-fraude.

Ces agents peuvent conduire une mission de diagnostic et de conseil pour faciliter le travail d'identification et de caractérisation des différents risques associés à leur champ d'expertise ; ils sont également susceptibles d'être consultés avec profit sur le degré de criticité de ces risques ainsi que le choix des mesures de maîtrise les mieux appropriées.

Des liens de coopération sont à envisager pour favoriser ces échanges, contribuer à la diffusion d'une culture de gestion des risques et plus généralement renforcer la professionnalisation des acteurs sur des questions éminemment transverses.

L'observation d'expériences passées ou en cours a notamment montré l'intérêt qu'il y a à opter pour des modes d'organisation souples et pérennes tels que la constitution d'un groupe projet dédié au déploiement de la démarche assurantielle à l'échelle de la collectivité ; cette solution se prête en outre aisément à la création de supports thématiques pluridisciplinaires (cahiers techniques pour l'évaluation des risques, spécifications fonctionnelles d'un système d'information dédié…) et à la mise en place d'un lieu ressource dématérialisé propre à capitaliser et mutualiser toute information d'intérêt commun.

Pour ce qui touche à la détection et à la prévention des risques de fraude et de corruption, la réflexion doit être menée en lien étroit notamment avec le référent déontologue de la collectivité, établi sur le fondement de l'article L 124-2 (issu de l'article 11 de la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires)[44].

Parmi les autres fonctions supports susceptibles d'être associées à la démarche on peut citer :

- le responsable qualité en tant que garant de l'assise méthodologique des travaux de collecte et d'évaluation ;
- le responsable conformité ;
- le chargé d'évaluation des politiques publiques au titre du pilotage de la performance ;
- le responsable de gestion budgétaire et financière ainsi que le directeur financier, plus particulièrement en anticipation d'une éventuelle exigence de certification des comptes ;
- le Délégué à la protection des données, qui s'assure de la correcte application des dispositions du Règlement général pour la protection des données à caractère individuel du 27 avril 2016 et de la loi Informatique et Libertés du 6 janvier 1978 modifiée ;
- l'inspecteur de l'action sanitaire et sociale, en charge de la prévention et qualité de vie au travail.

Il convient d'ajouter à cette liste les responsables des départements les plus directement engagés dans l'exercice de cartographie des risques, soit les Ressources humaines, les Services informatiques et notamment les agents dédiés aux questions de cybersécurité, les Affaires juridiques, les Affaires générales et le Patrimoine immobilier.

[44] Le référent déontologue peut être un agent de la collectivité ou une personnalité extérieure désignée à cet effet ; cette fonction est également susceptible d'être assurée par une instance collégiale ou sous-traitée à un centre de gestion.

1-B-3 Les instances de pilotage et de suivi

L'ampleur et l'étendue des questions soulevées par la mise en œuvre d'une démarche assurantielle globale appelle à la collégialité des décisions, sous réserve des points d'arbitrage touchant l'exposition au risque de la collectivité qui, dans tous les cas, doivent relever en dernier ressort de l'échelon politique.

De même, l'apport d'une expertise externe peut être bienvenu pour éclairer et documenter les choix de la gouvernance ; des demandes d'avis ponctuelles ou récurrentes peuvent ainsi être adressées à des personnalités qualifiées sélectionnées à cet effet.

De nombreux exemples montrent que ce type de consultation et d'échange est plus aisément réalisé dans le cadre d'un **Comité des risques** établi *ad hoc*[45].

Son rôle et ses missions peuvent être ainsi définis :

« *Le comité dédié au management des risques se réunit au moins une fois par an et assure une revue des principaux risques, en évaluant, pour chacun, l'évolution de sa criticité et de son niveau de maîtrise. Le comité des risques est chargé de la stratégie globale de gestion des risques et de la définition du niveau de tolérance en matière de risques, tant actuels que futurs. Il examine la mise en place opérationnelle des procédures en matière de contrôle des risques et des activités*. »[46]

Il appartient à chaque collectivité d'apprécier le besoin qu'il y aurait à créer en son sein une instance de cette sorte pour accompagner et renforcer la démarche prévue ou déjà engagée.

De même et selon l'organisation qui leur est propre, la Direction générale et l'exécutif pourront choisir de mettre concomitamment en place un Comité d'audit chargé d'évaluer le degré de maîtrise des risques identifiés ou au contraire de confondre ces travaux dans une seule instance qui aurait une vue générale sur la démarche assurantielle en cours - voir sur ce point la Section 3-B ci-après.

L'exemple d'un comité des risques

En accompagnement du déploiement d'une démarche assurantielle globale, une collectivité décide de créer une instance dédiée sous la forme d'un comité des risques.

Ce comité est composé de membres de l'exécutif, de la direction générale, du manager des risques et/ou du responsable de la fonction contrôle interne ; elle se réunit au moins une fois par an et à chaque évolution pouvant avoir un impact significatif sur la gestion des risques.

Au-delà du portage de la démarche, elle définit l'appétence aux risques en le formalisant dans un document validé par l'exécutif et la stratégie de management des risques.

En complément, il est apparu nécessaire de créer un comité opérationnel des risques associant la Direction générale et l'ensemble des directeurs. Cette instance a pour objet de soutenir le processus de management des risques et développer la culture du risque, à s'assurer de la mise à jour et du suivi de la cartographie des risques, à échanger sur les risques émergents et à veiller à l'élaboration et à l'avancement des plans de maîtrise pour les risques prioritaires.

[45] Voir les missions principales d'un Comité d'audit - Section 3-B (page 87) afin de déterminer son positionnement vis-à-vis du Comité des risques et d'établir leurs interactions possibles

[46] Maîtrise des risques dans les collectivités territoriales - Fiche relative au Principe n° 2 du cadre de référence du COSO-ERM 2017 (« Définir les structures organisationnelles ») - Publication conjointe CIAT-IFACI - 2019

2 Les prérequis d'une démarche de management des risques

Dans la section 1-A de cette publication il a été rappelé que les collectivités territoriales doivent répondre à une réglementation croissante, que ce soit dans les domaines techniques, financiers, juridiques, informatiques, ou relatifs aux ressources humaines.

L'expansion des contraintes réglementaires auxquelles sont soumises les collectivités territoriales a été à la mesure des nouvelles compétences qu'elles ont été appelées à exercer en réponse aux lois de décentralisation qui se sont rapidement succédé depuis près de quatre décennies.

La mission de ces collectivités territoriales est de délivrer des services publics qui permettent le fonctionnement de leur territoire et leur développement mais aussi de protéger la population qui y réside, son patrimoine ainsi que son environnement et ceci en toute circonstance.

Les décideurs mis à la tête de chacune d'entre elles se doivent ainsi de réunir les conditions d'un pilotage efficace et de donner pleine confiance dans l'action qu'ils mènent, ce qui passe par la conduite d'une démarche assurantielle reposant sur un dispositif complet de connaissance et maîtrise des risques associés à l'exercice de leurs responsabilités.

Or, la mise en place d'un dispositif de management des risques répondant aux normes en vigueur - telles qu'elles ont été rappelées dans la section 1-B - peut être perçue comme une tâche complexe ; une collectivité désireuse de s'y engager est nécessairement confrontée à la double question du périmètre qu'elle souhaite lui donner et - ce point étant établi - de son degré de détermination pour la mener à son terme.

En dehors des cartographies thématiques répondant à une nécessité réglementaire, il s'agit en effet d'une démarche volontaire qui doit apporter une réelle valeur ajoutée pour les parties prenantes et œuvrer comme un outil de facilitation dans l'atteinte des objectifs stratégiques et opérationnels de la collectivité.

Par conséquent, s'il n'y a pas d'adhésion à la démarche par les différents niveaux hiérarchiques, la démarche sera vouée à l'échec à un moment ou à un autre.

Comme pour tout système de management, cette adhésion doit être durable et portée par le plus haut niveau de la hiérarchie de la structure.

A cet égard, il est recommandé de procéder dans un premier temps sous la forme d'un groupe projet en charge d'une mission de préfiguration ; cette démarche sera étendue et pérennisée à mesure que seront atteints les objectifs intermédiaires et alors que les premiers succès rencontrés engageront à aller plus loin.

Ainsi, une démarche de management des risques doit être conçue comme un cheminement étape par étape, visant à l'intégration de la norme ISO 31 000-2018 selon des modalités et dans des proportions adaptées au contexte de chaque collectivité.

En particulier, et comme rappelé précédemment[47], une collectivité dépourvue d'une fonction d'audit interne a la possibilité de déployer un dispositif de gestion et pilotage des risques propre à fournir un degré d'assurance convenable sur sa capacité à contenir les principales menaces pesant sur son fonctionnement et la mise en œuvre des politiques dont elle a la charge ; ultérieurement et si le besoin en est établi, il lui reviendra de diligenter des travaux d'audit ponctuels ou récurrents notamment en vue de vérifier le degré de maîtrise des risques les plus critiques et de transformer une simple assurance donnée en une opinion d'audit parfaitement documentée et recevable à ce titre par des tiers.

[47] Voir Section 1-B-2

Dans cette optique, il est recommandé de réaliser une planification par phase, d'abord limitée à quelques objectifs modestes mais essentiels - comme la mise en place des cartographies ayant un caractère d'obligation réglementaire[48] - et de prévoir ensuite des objectifs plus ambitieux, qui seront d'autant mieux atteints que les succès obtenus dans les premières étapes auront conforté l'adhésion collective au projet d'ensemble.

Cependant, ces différentes étapes doivent être reliées par un fil conducteur menant vers un objectif global dûment concerté et conforme aux normes les plus généralement reconnues.

Aussi, la toute première étape à mettre en œuvre pour démarrer une démarche de management des risques consiste à faire un état des lieux afin :

- d'analyser le contexte interne et externe de la collectivité et plus généralement de son territoire;
- de mesurer le niveau de maturité en matière de management des risques au sein de l'organisation ainsi que sa culture ;
- de comprendre les attentes de l'exécutif et de la direction générale, leur sensibilité à la prise de risques ou à la saisie des opportunités afférentes ;
- d'inventorier les risques qui pourraient s'appliquer aux différentes activités exercées par la collectivité.

Ce diagnostic préalable est à présenter aux instances décisionnelles de la collectivité afin de vérifier leur accord pour engager une telle démarche, en pleine connaissance des moyens matériels et humains nécessaires à son exécution ainsi que des choix stratégiques éventuels induits par une approche prudentielle des risques.

Par souci de transparence et afin d'écarter toute possibilité de malentendu futur, le rapport d'arbitrage établi dans ce sens doit mettre en avant les points forts de la collectivité ainsi que les points d'attention ou d'amélioration notamment vis-à-vis des enjeux et des objectifs à atteindre.

De même, il importe que les éléments présentés ou produits à l'issue de cette phase préparatoire soient systémiquement issus d'une réflexion collective, de sorte qu'ils puissent être objectivés, quantifiés et - dans la mesure du possible - documentés.

Sur ce point, Il peut être utile d'intégrer très tôt des experts métiers dans le groupe projet, voire même dès la phase de préfiguration, afin de consolider les fondements techniques des travaux menés et de mieux asseoir leurs conclusions et recommandations.

Enfin, le choix de la période de lancement de la démarche n'est pas sans incidence sur son déroulement et sa bonne fin.

De manière générale, il est préférable qu'elle intervienne en début de mandat ou tout du moins dans le cours de la première moitié du mandat.

Les commencements d'un projet administratif et politique engageant l'avenir du territoire se prêtent en effet particulièrement à un exercice de cartographie des risques majeurs qui y sont associés ainsi que des opportunités sous-jacentes.

Ce chantier permet de donner connaissance au nouvel exécutif du degré global de vulnérabilité de la collectivité et, le cas échéant, de ses points de fragilité particuliers.

Par ailleurs, il peut être intéressant d'en tirer profit pour faire un inventaire des incidents marquants intervenus dans un passé proche (cinq à dix années par exemple), ceci afin d'attirer l'attention sur la nécessité d'agir sur les risques et d'identifier plus précisément les principales zones d'exposition de la collectivité.

Dans tous les cas, les fins de mandats ne sont pas propices au lancement d'un projet de cette envergure, à moins de préparer une méthodologie pour un projet à présenter au mandat suivant.

[48] Par exemple la cartographie des risques de fraude en application de la loi « Sapin 2 » du 9 décembre 2016

La cartographie des risques, élément pivot

La cartographie des risques constitue l'élément central du dispositif de management des risques.

Au-delà de la vision d'ensemble qu'elle offre, elle témoigne à tout moment du niveau de maîtrise des risques de la collectivité et facilite l'implication des parties prenantes.

Le succès d'une cartographie des risques réside dans son utilisation effective, dans sa contribution réelle à l'aide à la décision et à la gestion des risques, mais également dans la capacité des utilisateurs à la faire vivre et évoluer dans le temps.

A cet égard, il convient de souligner l'importance d'une démarche itérative inscrite dans la durée.

Une collectivité est en effet peu susceptible de mettre en place une cartographie répondant à ses besoins et attentes avant quelques années : il est préférable qu'elle mesure ses ambitions au départ et ne se décourage pas face à des démarches trop lourdes et complexes.

Pour y parvenir, différentes approches sont présentées dans la Section 2-B ci-après.

Quelle que soit la méthodologie retenue, cet exercice nécessite préalablement de bien apprécier la culture de la collectivité, ainsi que ses niveaux de maturité et d'appétence pour le risque.

Qu'est-ce qu'une cartographie des risques ?

Ce terme désigne l'ensemble des données propres à décrire et piloter les risques auxquels une collectivité est exposée du fait de son fonctionnement et de la mise en œuvre des politiques dont elle a la charge.

Une cartographie est ainsi généralement composée des éléments suivants :

- un corpus de fiches décrivant les risques identifiés (facteurs de risques, impacts potentiels, dispositifs de maîtrise existants, faits avérés et retours d'expériences) ;
- un processus continu d'évaluation permettant d'identifier les risques majeurs qui pourront donner lieu à un suivi/traitement prioritaires du fait de leur criticité et de leur niveau de maîtrise perçu ;des représentations graphiques sous forme de matrices conçues pour une communication efficace et itérative.

L'outil décisionnel ainsi constitué a pour objet de documenter une vue d'ensemble sur le degré d'exposition de la collectivité à la possibilité de survenance d'évènements propres à compromettre son fonctionnement quotidien - voire même la continuité du service rendu aux usagers - ainsi que sur l'efficience des mesures de maîtrise qui y répondent.

Les représentations graphiques adoptées pour une cartographie des risques prennent généralement la forme :

- d'un radar en forme de roue - aussi appelé diagramme de Kiviat, ou graphique toile d'araignée - permettant de visualiser le degré de criticité des risques prioritaires identifiés compte tenu et non tenu des mesures de maîtrise afférentes ;
- d'un graphique à deux entrées - dit Matrice de Farmer - représentant le positionnement des risques au regard des deux facteurs qui déterminent leur criticité respective, soit leur probabilité et leur impact évalués en abscisse et en ordonnée, avec ou sans l'effet des mesures de maîtrise qui se rapportent à chacun d'entre eux.

D'autres modes de représentation peuvent être adoptés, en particulier de manière à faire apparaître le rapport entre la criticité de chaque risque et l'importance (donc le coût) des mesures de maîtrise correspondantes, selon le schéma MARCI présenté dans la Fiche technique n° 16.

2-A Les conditions du succès

En amont du déploiement d'une démarche globale de management des risques, une collectivité peut trouver avantageux de conduire une mission de préfiguration dans le but de vérifier que les facteurs de succès de la démarche sont effectivement réunis.

Dans le cas où il apparaîtrait que ces conditions ne sont pas suffisamment remplies, les instances dirigeantes de la collectivité auront l'option de planifier et mettre en œuvre une phase de transition vers un mode de management et de fonctionnement mieux à même de répondre aux besoins du projet.

La transformation de la collectivité dans le sens d'une organisation plus réactive et résiliente est d'ailleurs une condition autant qu'une conséquence de la mise en œuvre d'un processus structurant de pilotage des risques à visée stratégique et assurantielle.

Il s'agit d'un mécanisme vertueux où chaque composante concourt à la bonne fin de travaux engagés concurremment et s'inscrit dans une trajectoire de progrès au bénéfice de l'ensemble du territoire.

Il est recommandé de focaliser ce travail exploratoire sur les points suivants.

2-A-1 Evaluer l'environnement externe

Cette première étape vise à comprendre l'environnement dans lequel s'inscrit la collectivité, les leviers qu'il offre pour la conduite du projet et les freins potentiels contenus dans telle ou telle de ses spécificités.

Pour appréhender ce contexte externe et en tirer les enseignements attendus, la collectivité peut recourir à plusieurs méthodes.

La méthode dite de PESTEL paraît être la mieux appropriée à ce dessein dans la mesure où elle balaye globalement l'ensemble des facteurs influençant les orientations d'un mandat territorial et du projet d'administration sous-jacent.

En déroulant l'acronyme qui désigne la méthode, il s'agit de déterminer le contexte Politique, économique, social, technologique, environnemental et légal (PESTEL) de la collectivité justifiant la mise en place d'une cartographie des risques et la conduite d'une démarche assurantielle globale.

A cette liste, il pourrait d'ailleurs être approprié d'ajouter une dimension sanitaire - qui pourrait être rapprochée des thématiques environnementales - du fait de son possible impact sur la conduite des politiques territoriales et les contraintes qui les déterminent.

Dans chacune de ces thématiques, la collectivité est appelée à définir les éléments qui pourraient relever d'un risque ou d'une opportunité en fonction des compétences portées.

De même, une veille régulière de ce contexte externe sera riche d'informations pour garantir une vision globale des risques et alerter sur l'évolution ou l'émergence de nouvelles menaces ou opportunités éventuelles.

Ce travail permettra également de commencer à construire l'univers et le référentiel des risques le mieux adapté aux besoins et au contexte de la collectivité.

2-A-2 Evaluer l'environnement interne

Parallèlement à l'analyse de son environnement, une collectivité désireuse de s'engager dans une démarche de gestion prévisionnelle des risques doit s'assurer que les voyants sont au vert en interne - ou tout du moins ne sont pas ouvertement au rouge - sur les trois aspects essentiels que sont la maturité, la culture et l'appétence aux risques.

Maturité

Pour évaluer la maturité d'une collectivité sur la question des risques, il y a lieu de comprendre son organisation et son fonctionnement au regard des points suivants :

- l'existence ou non de cartographies des risques quelles qu'elles soient (risques majeurs, protection des données à caractère personnel, risques d'atteintes à la probité, aléas/vulnérabilité aux risques naturels, risques informatiques et cybersécurité, risques RH, risques liés à l'utilisation de financements européens…) ;
- la mise en place de deux à trois lignes de maîtrise des risques clairement identifiées et agissant en interaction[49] ;
- le positionnement des différents métiers gérant des risques spécifiques (lutte contre la fraude, mise en œuvre des crédits de la politique européenne de cohésion, protection des données à caractère personnel, cybersécurité…) ou ayant mis en place des dispositifs de réponse à la gestion de certains risques pour la collectivité ou le territoire (dispositif de gestion des crises, des risques naturels…).

En complément de ces points, il convient de rechercher l'état d'avancement de la réponse de la collectivité aux obligations réglementaires qui lui sont imposées.

Plus généralement, la revue documentaire et méthodologique préalable au lancement du projet doit donner des indications suffisantes sur :

- les services ou les directions qui sont certifiés ou qui sont engagés dans une démarche de certification ;
- les services ou les directions qui ont part à un projet de management quel qu'il soit (qualité, sécurité, environnement, énergie, anticorruption…) ;
- les référentiels et autres documents structurants en usage dans l'administration, sous forme de chartes, de guides, de procédures…

Pour le cas ou des cartographies des risques partielles seraient déjà mises en place, l'exercice doit permettre d'identifier le ou les pilote(s) de ces démarches ainsi que les modalités de collecte et de suivi retenues.

Toujours dans cette hypothèse, il peut être opportun d'interroger les pilotes sur la méthodologie employée (grille de cotations, vocabulaire utilisé…) ; la valorisation de ce travail et sa pleine articulation avec la démarche envisagée sont des facteurs importants d'adhésion sur le long terme et constituent des gages de succès pour le travail à mener, tant celui-ci repose sur la qualité des coopérations internes et externes.

[49] Voir plus haut Section 1-B-1

En s'aidant de ces informations, la collectivité est ainsi en mesure :

- d'apprécier le périmètre de couverture de la démarche assurantielle, ses incidences sur l'organisation et le fonctionnement de la collectivité ainsi que les délais nécessaires à la bonne fin du projet;
- d'identifier les acteurs des démarches les plus avancées qui seront de précieux appuis pour les travaux à venir (par exemple sous la forme de groupes pilotes sollicités dans les premières étapes du processus global).

S'ils sont présents et conformes aux standards attendus, les éléments préparatoires évoqués ici sont autant de briques déjà prêtes pour établir rapidement et solidement les fondations du projet.

A l'inverse, s'il apparaît qu'ils sont manquants ou insuffisamment aboutis, la collectivité devra planifier leur mise ou remise à niveau à mesure que se déploiera une démarche assurantielle de contrôle et de gestion des risques.

Culture

La culture de la collectivité est un autre élément clé qui doit être étudié avec précision préalablement au démarrage du projet, dans la mesure particulièrement où elle influera sur la méthodologie retenue pour la conduite des différents travaux de management des risques.

Il s'agit d'un concept protéiforme qui doit être utilisé avec prudence et en tenant le plus grand compte de chaque contexte particulier.

Ainsi, la culture d'une collectivité peut notamment se déceler dans sa manière de :

- traiter les dossiers (circuit de validation ou d'arbitrage, poids des services supports…) ;
- conduire le changement organisationnel ou autre ;
- manager les équipes (management en silo, en transversalité) ;
- innover tant dans la mise en place d'outils de gestion, d'accompagnement que dans la conduite même de projet innovant propre à chaque métier… ;
- tisser et entretenir son réseau partenarial ;
- structurer sa gouvernance interne tant pour l'administration que pour l'exécutif.

La taille de la collectivité, la pluralité de ses compétences et de ses métiers sont également à prendre en considération.

De même, la culture de la collectivité n'est pas sans lien avec les traits marquants de son ressort territorial, le profil individuel de ses dirigeants ainsi que son histoire ; à cet égard il est important de rechercher les événements passés qui ont pu déterminer la manière présente d'aborder le risque, tant en termes de menaces que d'opportunités, et plus généralement la philosophie présente dans l'exercice de ses responsabilités.

Le traitement qui a été fait de ces épisodes anciens et les conséquences de cette gestion sur le plan humain, financier, juridique, technique ou réputationnel influeront nécessairement l'appréhension des futurs événements et donc la prise en compte des risques afférents.

Enfin, le diagnostic intrinsèque de la maturité de chaque direction ou service au regard des enjeux et modalités d'une gestion prévisionnelle des risques est un élément constitutif de la culture de la collectivité.

Le degré particulier d'avancement des diverses composantes de l'administration territoriale doit amener à aborder différemment la démarche de management des risques :

- les directions ou acteurs ayant d'ores et déjà une approche par les risques pourront en tirer avantage pour créer des ponts entre leur culture métier et une approche plus large (lien entre les grilles de cotations, correspondance entre le vocabulaire technique métier et celui des risques dans une démarche assurantielle globale…) ;
- les directions ou acteurs disposant d'un système de management formalisé et éventuellement adossé à des normes ISO ou autres pourront s'appuyer sur la cartographie des processus, des risques et opportunités identifiés et les plans d'action subséquents pour renforcer leur méthodologie de travail et acquérir de nouveaux outils d'analyse ;
- les directions ou acteurs novices devront plutôt être abordés sous l'angle de la sensibilisation, notamment au travers de l'analyse des difficultés éventuellement rencontrées dans la réalisation de leurs objectifs et des opportunités non exploitées susceptibles au contraire de faciliter la bonne fin des opérations dont ils ont la charge, ces échanges doivent témoigner de l'intérêt de la démarche et apporter une aide dans la recherche de solutions adaptées.

Ces éléments seront riches d'enseignement pour la collectivité qui pourra en tirer parti pour conforter ou éventuellement faire évoluer ses procédures.

Ils permettront de définir les approches les mieux adaptées pour aborder la gestion des risques et de choisir un langage adéquat pour faciliter les échanges et susciter l'adhésion des différentes parties concernées.

En effet, même si l'appréciation des risques doit être la plus neutre possible, il peut subsister des biais cognitifs dans le choix des risques prioritaires à traiter et la détermination de leur niveau de maîtrise.

Bien entendu et selon le diagnostic réalisé, il conviendra d'adapter cette méthode en fonction de la culture de chaque direction ou service de la collectivité.

Ainsi une certaine approche pourra donner entière satisfaction dans une direction et moins dans une autre car leurs cultures respectives seront très éloignées.

Pour approfondir le sujet…

Le principe n° 3 du cadre de référence du COSO-ERM 2017 a pour titre « Définir la culture souhaitée » et se définit comme suit : « *L'organisation définit les comportements attendus qui caractérisent la culture souhaitée par l'entité.* »

Des conseils et méthodes pour la mise en application de ce principe sont proposés dans les Fiches pratiques publiées par la CIAT et l'IFACI en 2019 sous le titre « *La Maîtrise des risques dans les collectivités territoriales* ».

A titre d'exemple, parmi les bonnes pratiques citées, celles-ci font écho aux recommandations qui précèdent : « *Faire en sorte que la culture de l'organisation influence la manière dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs de l'organisation. Veiller à ce que la gestion du risque, de son identification à son évaluation, en passant par son traitement, soit en conformité avec la culture de l'administration.* »

Appétence

L'appétence aux risques se définit comme le niveau de risque qu'une collectivité est disposée à prendre au regard du coût induit par un renforcement des moyens de maîtrise ou même la suppression de tout ou partie des menaces résiduelles.

Ce niveau se situe au point de basculement entre des opportunités à saisir - du fait de l'acceptation du risque - et les conséquences éventuelles de la survenance de l'événement considéré qui doivent être absolument écartées dans la mesure où elles impactent des aspects cruciaux du fonctionnement de la collectivité et/ou de la mise en œuvre des politiques dont elle a la charge.

Ce point de rupture peut être difficile à situer voire à formaliser s'agissant de missions de service public rendues à la population.

De manière générale une approche prudente et circonstanciée est de mise.

Dans le cas de la lutte anti-corruption, les collectivités sont invitées à porter un objectif de tolérance zéro qui doit se comprendre comme le compas des politiques menées et la traduction ultime de l'engagement affiché de l'instance dirigeante [50]

En conséquence, les risques relatifs à l'éthique et à la compliance déontologique doivent faire l'objet des soins les plus attentifs et mobiliser en priorité les moyens de maîtrise et de de contrôle à la disposition de la collectivité.

A l'inverse, des critères de décision objectifs et aisément ajustables peuvent être adoptés en matière financière ; à partir des comptes administratifs et quelques indicateurs financiers clés - tels que le taux d'endettement, la durée de désendettement, la capacité d'investissement, le poids de la fiscalité… - il est en effet possible de définir un niveau de prise de risques acceptable, c'est-à-dire situé en-deçà de maxima qui conduiraient à des situations irréversibles.

En toute hypothèse, la détermination de l'appétence aux risques d'une collectivité revient exclusivement à ses instances dirigeantes et en premier lieu à l'Exécutif car il s'agit de décisions éminemment stratégiques sinon politiques qui engagent ses valeurs et fixent sa trajectoire sur le long terme. Tout particulièrement en début de mandat, le fait de travailler sur cette notion peut mettre en évidence des divergences de points de vue parmi les élus ou une majorité constituée mais elle aussi peut être une force d'alignement qui permet de partager et traduire les grands intérêts communs.

Il convient en outre de ne pas confondre l'appétence aux risques avec la tolérance qui est la marge de manœuvre propre à chaque direction ou service à l'intérieur même du cadre d'appétence.

Enfin, il peut être utile d'étendre l'appétence aux risques à une approche par les opportunités afin de mieux rendre compte de l'étendue des arbitrages qui se présentent à l'exécutif de chaque collectivité.

Pour approfondir le sujet…

Le principe n° 7 du cadre de référence du COSO-ERM 2017 a pour titre « *Définir l'appétence pour le risque* » et se définit comme suit : « *L'organisation définit l'appétence pour le risque dans le contexte de la création, de la préservation et de la concrétisation de la valeur*».

Des conseils et méthodes pour la mise en application de ce principe sont proposés dans les Fiches pratiques publiées par la CIAT et l'IFACI en 2019 sous le titre « *La Maîtrise des risques dans les collectivités territoriales* ».

[50] Voir Section 1-A-1 supra

Identifier et représenter les risques comme des menaces autant que des opportunités

Comme rappelé précédemment, le risque est défini par la norme ISO 31000 comme étant « *l'effet de l'incertitude sur les objectifs* [d'une organisation] » sous réserve de comprendre qu'un effet est un « *écart par rapport à un attendu* [qui] *peut être positif, négatif ou les deux à la fois et traiter, créer ou entrainer des opportunités et des menaces* ».[51]

Or force est de constater que dans les démarches de management des risques, la traduction des menaces est prédominante.

Dans leur écrasante majorité, les cartographies et les matrices représentent les impacts négatifs tant en gravité qu'en probabilité.

Le même principe peut toutefois s'appliquer aux opportunités.

En lieu et place de matrices représentant les probabilités de survenance de tel ou tel événement en fonction de la gravité, les collectivités peuvent ainsi faire le choix de mesurer leur intérêt au regard de la valeur ajoutée apportée.

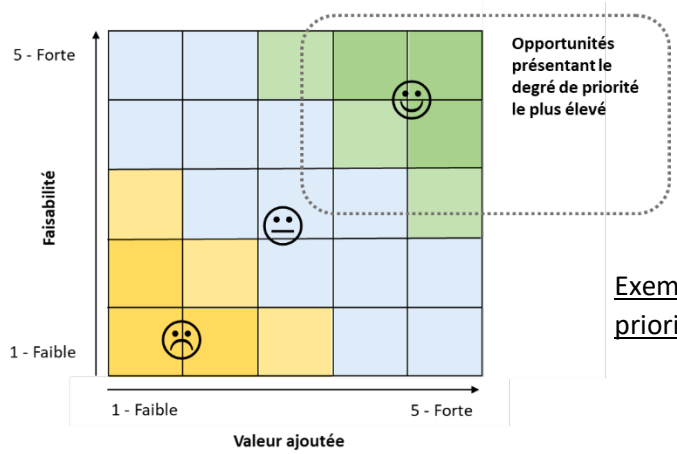
De la même façon que l'évaluation d'un risque, des échelles de cotation des opportunités peuvent être établies de manière à mesurer :

- leur faisabilité (technique, réglementaire, financière, de gouvernance voire d'acceptabilité sociétale par exemple) ;
- la valeur ajoutée apportée en termes financiers, opérationnels, réputationnels…. ces critères devant être en cohérence avec les orientations politiques du mandat et le projet d'administration qui en résulte.

De la même façon que pour les mesures visant à prévenir et/ou contenir des événements négatifs, la Direction générale et l'Exécutif seront appelées à identifier des opportunités présentant un caractère de priorité et à diligenter des actions visant spécifiquement à améliorer la faisabilité ou à augmenter la valeur ajoutée.

Ce faisant, une collectivité pourrait établir une cartographie commune des risques et des opportunités associées.

La notion d'opportunité ainsi affirmée contribue à une approche positive du management des risques et permet de donner des risques une image plus large et plus attractive que la simple représentation de menaces potentielles.



Exemple de matrice pour guider la priorisation des opportunités relevées

[51] Voir Section 1-B - Propos préliminaire

2-B Choisir un mode opératoire

En appui du résultat de ces investigations et après avoir précisément établi le contexte de la démarche, les instances dirigeantes de la collectivité seront amenées à définir la méthodologie la mieux adaptée à leurs besoins spécifiques ; ce choix doit être réalisé avec le souci d'approcher les risques en construisant une cartographie juste et partagée par les futurs acteurs de leur maîtrise.

En effet, les étapes préparatoires ne se limitent pas à la vérification de la capacité de la collectivité à porter un projet structurant de cette importance ; il faut encore en mesurer toutes les incidences organisationnelles et réunir effectivement les ressources nécessaires à son maintien dans la durée.

A ce point d'avancement de sa réflexion, la collectivité est ainsi amenée à trancher quelques points clés de méthode qui détermineront la nature et l'importance travaux à mener.

Puis-je réaliser plusieurs cartographies des risques au sein de mon organisation ?

Le découpage éventuel de la cartographie des risques de la collectivité dépendra du degré d'information souhaité :

- au niveau stratégique (direction générale) si l'on recherche une vision générale des risques dans la collectivité ;
- au niveau fonctionnel ou opérationnel si l'on souhaite une vision claire des risques au sein de chaque Direction ou service ;
- sur un domaine particulier pour obtenir une vision spécifique des risques sur un sujet, par exemple les atteintes à la probité ou dans le domaine informatique.

Dans tous les cas et afin que le management des risques soit intégré, structuré, global - ainsi que le demande la Norme 31000-2018[52] - il importe que les cartographies thématiques soient consolidables sur le modèle de la cartographie générale ou au contraire que la cartographie générale soit divisible en cartographie thématiques mais toujours avec le même souci d'une homogénéité et d'une structuration communes.

A quelle échéance dois-je renouveler l'exercice ?

La cartographie doit être suivie, révisée et complétée régulièrement pour intégrer les évolutions, les changements et l'émergence de nouveaux risques.

Si l'on se place dans l'optique de mandats électifs, il est recommandé de réaliser deux exercices complets par mandat (par exemple, en fin de mandat pour constituer un outil de préparation à destination de la gouvernance en début du nouveau mandat, puis à mi-mandat), complété de mises à jour annuelles sur la base des actualités réglementaires ou politiques, et de faits particuliers (condamnation de la collectivité, nouvelle délégation de service public...).

[52] Voir supra, Section 1-B-1

2-B-1 Trouver la meilleure entrée pour l'identification des risques

En tout premier lieu, il convient de rappeler que, même si le risque zéro n'existe pas, il est important d'évoluer dans un environnement où les risques sont acceptables.

Cependant identifier les risques acceptables revient pour les instances dirigeantes à connaître précisément leurs conséquences et avoir la capacité de les assumer en pleine connaissance de cause.

A cet effet, plusieurs approches pour identifier les risques sont possibles, parmi lesquelles trois émergent.

Entrée	Descriptif
Par les objectifs	Il s'agit d'identifier les objectifs stratégiques de l'entité, de recenser les risques propres à compromettre leur atteinte, puis de déterminer éventuellement les contrôles et mesures de réduction à mettre en place.
Par les risques	Cette approche se distingue de la précédente par le fait qu'il s'agit d'identifier dans un premier temps, pour l'ensemble du périmètre étudié, les risques les plus importants pouvant compromettre les objectifs fixés. Pour cela, il est possible de partir des risques avérés en faisant le recensement des incidents qui se sont déjà produits, puis de compléter par une réflexion sur les risques potentiels et inhérents à l'activité.
Par les processus	Cette méthode est plus minutieuse et nécessite un travail préparatoire conséquent. Il s'agit de décomposer la collectivité en processus et sous processus et de comprendre les objectifs qui y sont associés. Ensuite, avec les acteurs concernés, le travail consiste à identifier les risques par processus de non atteinte des objectifs opérationnels.

Ces différentes entrées ne sont pas exclusives l'une de l'autre et peuvent être utilisées conjointement ou même successivement, à mesure que progressera la démarche.

Ainsi l'approche par les risques peut être un choix avantageux pour une collectivité encore peu familière de ces questions car elle permet l'agrégation empirique d'éléments contribuant à un schéma-cible peu contraignant et évolutif ; cette façon d'opérer est parfaitement viable dès lors qu'une base méthodologique minimale a été d'abord établie, notamment pour ce qui touche au périmètre de l'exercice, aux familles de risques constitutives de ce périmètre ainsi qu'aux modes de collecte et de validation des informations requises.

Par ailleurs, l'approche par les processus est souvent plus familière aux collectivités déjà engagées dans une démarche qualité.

Elle présente l'avantage d'être indépendante des changements de structure, puisque s'appuyant sur des procédures validées et appliquées par tous, et de reposer sur une importante quantité de ressources documentaires.

De même, elle permet d'identifier aisément les responsabilités.

Enfin, elle se prête particulièrement à la conduite de travaux d'audit et favorise la mise en œuvre d'un programme d'audit à l'échelle de la collectivité, lequel constitue la pierre faîtière d'une démarche assurantielle globale.

Reconnaître les processus métiers de la collectivité

Comme on l'a vu, l'approche par processus consiste à décomposer la collectivité en processus et sous processus et en comprendre les objectifs opérationnels.

Cet exercice de représentation prend en principe la forme d'un diagramme de flux.

Le diagramme de flux vise à représenter graphiquement le déroulement d'un processus au travers des éléments suivants :

- enchaînement chronologique des activités ;
- identification des acteurs en charge de ces activités ;
- représentation des flux d'informations d'une activité à l'autre.

Cet outil permet d'identifier les risques relatifs à chaque activité du processus et les contrôles clefs concourant à leur maîtrise.

Toutefois, afin d'éviter un travail préparatoire trop important et chronophage, il est possible de s'en tenir à la modélisation simple d'un macro-processus (phases, tâches, acteurs, outils).

Ce macro-processus servira ensuite de base de travail à l'identification des risques.

Exemple : La gestion et l'attribution des subventions

Un processus peut être décrit sans qu'il y ait besoin de recourir à une modélisation détaillée (ex : diagramme de flux) ; un descriptif succinct des tâches constitutives de la chaine de traitement peut s'avérer être un support suffisant pour l'exercice demandé.

Dans l'exemple donné ici, le processus de gestion et d'attribution des subventions est segmenté en six phases successives (demande, instruction, décision, paiement, contrôle, publicité et archivage) et chacune des phases est elle-même divisée en tâches principales, à raison de deux à sept tâches par phase.

Pour chacune des tâches ainsi identifiées, il y a lieu de spécifier les outils (logiciels en particulier) utilisés ainsi que les acteurs impliqués.

Phases	Demande		Instruction							Décision						Paiement		Contrôle			Publicité et Archivage	
Tâches	Diffusion d'un appel à projets	Dépôt du dossier de demande	Réception du dossier de demande	Vérification de la complétude du dossier	Le cas échéant, demande des pièces manquantes	Analyse d'éligibilité de la demande	Analyse de la situation financière du demandeur	Rédaction du rapport d'instruction	Réalisation et contrôle des cahiers de subvention	Etude des cahiers en commissions thématiques	Élaboration du rapport, de la délibération et de la convention	Décision de l'assemblée délibérante	Transmission au contrôle de légalité	Envoi des courriers de notification	Signature de la convention	Vérification des conditions de versement	Mandatement	Envoi des documents bilans	Contrôle de l'utilisation de la subvention	Evaluation du dispositif subventionné	Publicité des subventions versées	Archivage du dossier
Outils																						
Acteurs																						

Construire et alimenter un diagramme de flux

Le diagramme de flux (*flowchart*) vise à représenter graphiquement le déroulement d'un processus.

Préalablement à sa création, il convient de réunir ses différents éléments constitutifs en procédant selon les cinq étapes :

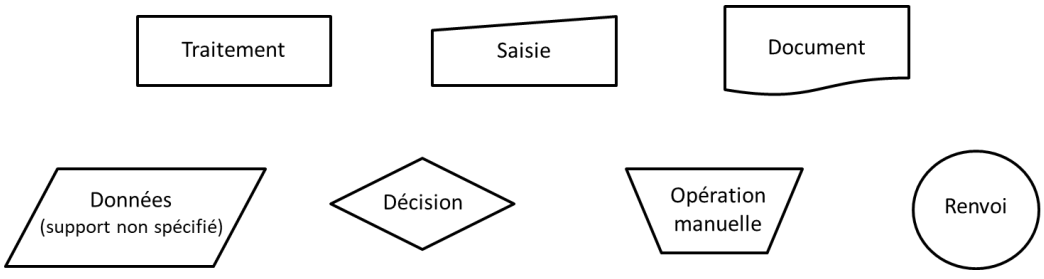
- Identification du processus à représenter ;
- Identification des activités composant le processus ;
- Identification des acteurs en charge de ces activités ;
- Identification des documents associés à chacune de ces activités (élément conditionnant l'entrée ou la sortie comme une délibération, un bon de commande, un bon de réception…) ;
- Identification des flux.

Pour la dernière étape, afin de représenter les flux associés à chacune des activités identifiées, il est nécessaire de réaliser un tableau faisant apparaitre :

- en entrée, le récepteur ainsi que la ou les condition(s) de réception (mise à disposition de pièces, d'informations avant traitement…) ;
- en sortie, l'émetteur ainsi que la ou les condition(s) d'émission (mise à disposition de pièces, d'informations après traitement…).

Activités associées au processus	Entrées		Sorties	
	Récepteur	Conditions	Emetteur	Conditions

Dans l'élaboration des diagrammes de flux, il est recommandé de faire usage des symboles issus de la Norme ISO 5807, soit en particulier les figures suivantes.



Il peut être aussi recommandé d'utiliser le langage BPMN (Business process model & notation), langage de modélisation standard actuel pour concevoir des processus métier dont les principaux symboles sont utilisés dans la plupart des logiciels de modélisation de processus.

2-B-2 Collecter et agréger les données disponibles

Ensuite et quelle que soit l'approche choisie, il est nécessaire d'opter pour une démarche appropriée de collecte de d'agrégation des éléments constitutifs de la cartographie des risques :

- une démarche « montante » (*bottom-up*) qui permet d'avoir une vision proche de la réalité puisqu'il s'agit de partir du terrain. Mais il y a un risque de non-rapprochement avec la politique et les objectifs définis ;
- une démarche « descendante » (*top-down*) qui à l'inverse de la précédente permet d'être en cohérence avec la politique et les objectifs définis mais risque d'être théorique ;
- une démarche mixte qui est une combinaison des deux approches.

De manière générale, il est souhaitable de ne pas retenir une des deux premières méthodes sans utiliser les garde-fous nécessaires pour ne pas basculer dans un exercice anarchique ou au contraire excessivement verrouillé.

A cet égard, dans les Fiches pratiques publiées par la CIAT et l'IFACI en 2019 sous le titre « *La Maîtrise des risques dans les collectivités territoriales* » il est fait mention de deux écueils à éviter :

« *Adopter une approche bottom-up sans filtre ni consolidation : tous les risques identifiés et suivis par le management opérationnel remontent vers la direction générale dans un portefeuille trop exhaustif pour être piloté* [ou] *Retenir une approche strictement top-down : la direction générale ne demande à être informée que des risques qu'elle a elle-même pré-identifiés comme intéressant à son pilotage stratégique*. »[53]

Par ailleurs, pour une meilleure visibilité et une efficacité accrue, il est recommandé que le pilotage de la démarche revienne à un agent nommément désigné, en charge d'une mission de préfiguration précisément déterminée quant à son objet, ses modalités de réalisation et sa durée.

En outre, cet agent trouvera avantage à être directement rattaché à la Direction générale ou à un directeur / directeur général adjoint en charge des fonctions support, ceci de manière à disposer de la transversalité nécessaire à la conduite d'un tel chantier.

2-B-3 Déterminer le périmètre de l'exercice

Enfin, la collectivité doit se poser la question de l'étendue du chantier qu'elle entend mener à bien, sous l'angle du périmètre de la cartographie des risques attendue comme livrable final.

Un bloc de risques endogènes se retrouvent peu ou prou dans l'ensemble des collectivités et il lui faut de prime abord y rechercher les fondements de la cartographie en construction.

De même, l'intégration des risques liés aux dysfonctionnements d'organismes satellites de la collectivité a un caractère de quasi-obligation dans le domaine de la lutte anti-corruption ou en matière comptable et financière.

Au-delà de ce socle commun, il lui faut en outre se déterminer à inclure - ou non- les catégories suivantes :

- les risques liés à des défaillances de fournisseurs et sous-traitants ;
- les risques exogènes hors du périmètre direct de la collectivité.

[53] Voir la Fiche technique rattachée à la recommandation n° 14 du cadre de référence du COSO-ERM 2017 « Développer une vision globale du portefeuille de risques »

Les risques endogènes associés auxquels se trouve exposée une collectivité peuvent être classés en appui des catégories proposées dans le COSO-ERM 2017[54] au regard des différents métiers qui se trouvent en son sein.

En dépit de la grande diversité des situations, certains aspects communs se retrouvent aisément.

Les risques comptables et financiers constituent une première famille aisément identifiable : leur caractère d'homogénéité est également un facteur facilitant de suivi et de pilotage.

En effet, une situation comptable ou financière défavorable est de nature à priver une collectivité des moyens d'agir et entraîne quasi-certainement la non-réalisation des objectifs contenus dans le projet de mandat ; ce type d'événement a ainsi un impact majeur sur l'ensemble des politiques menées et même sur la capacité de l'organisation à maintenir un fonctionnement satisfaisant.

A titre d'exemple, les risques comptables et financiers suivants peuvent être évalués :

- une dérive des dépenses ;
- la non obtention de recettes attendues ;
- une politique d'emprunt non optimale.

Par ailleurs et comme rappelé précédemment, l'expérimentation de la certification des comptes des collectivités conduite sur le fondement de l'article 110 de la loi NOTRe a montré la nécessité d'établir une cartographie des risques comptables et financiers pour donner une assurance raisonnable quant à la fiabilité et l'efficience des procédures de gestion sous-jacentes[55].

Les risques liés à la mise en œuvre des crédits de la politique européenne de cohésion constituent une variété particulière de risques comptables et financiers, dans la mesure notamment où les collectivités exerçant les responsabilités dévolues à l'autorité de gestion d'un ou plusieurs programmes - à titre principal ou délégué - s'exposent à des corrections financières en cas de mésusage de ces financements.[56]

En second lieu, les risques liés à la réalisation d'actes contraires à la probité sont appelés à se retrouver, à des degrés divers, dans l'ensemble des collectivités.

Ces risques ont souvent un impact comptable et financier mais leur incidence est bien plus grande en ce sens qu'ils ont des aspects réputationnels, juridiques et humains sans commune mesure avec les conséquences de simples erreurs matérielles ou de comportements négligents.

Comme cela a été précédemment indiqué, l'Agence française anti-corruption (AFA) fait obligation à chaque collectivité locale d'établir une cartographie des risques de fraude en son sein[57].

Cet exercice peut constituer le point de départ d'une cartographie des risques étendue aux différents aspects du fonctionnement de la collectivité et à la mise en œuvre des politiques dont elle a la charge.

Dans tous les cas, il est recommandé de traiter les risques de corruption comme une catégorie à part entière, du fait de leur caractère de transversalité et aussi parce que la collectivité sera éventuellement appelée à en rendre compte auprès de l'AFA[58] (ainsi que des instances de contrôle et/ou d'audit de la Commission européenne s'il elle est responsable de la mise en œuvre de crédits communautaires).

[54] Voir supra, Section 1-A - Points préliminaires

[55] Voir supra, Section 1-A-3 et Fiche technique n° 4

[56] Voir supra, Section 1-A-1 et Fiche technique n° 3

[57] Voir supra, Section 1-A-1 et Fiche technique n° 2

En troisième et dernier lieu, une collectivité sera conduite à appréhender différentes catégories de risques touchant au maintien des fonctions support essentielles - ressources humaines, informatique, affaires réglementaires, bâtiments et logistique - mais aussi à sa capacité à délivrer les services aux usagers qui sont attendus de sa part et plus généralement à mener à bien les politiques dont elle a la charge.

Ces types de risques sont fort nombreux et chaque collectivité est parfaitement fondée à établir sa propre nomenclature, qui répondra à son contexte, à ses besoins spécifiques et à sa culture particulière.

Toutefois, quelques pistes peuvent être données ici à titre d'illustration.

Ainsi, on peut citer comme exemples de risques liés aux ressources humaines :

- une allocation non optimale des moyens humains ;
- une montée des préjudices subis par les personnels ;
- une recrudescence des absences au travail ;
- une extension des conflits sociaux.

Parmi les risques liés aux Systèmes d'information, on peut notamment retrouver :

- l'action de logiciels malveillants, des actes de piratage, des intrusions de compte ;
- des pertes de données par défaut de sauvegarde ou des préjudices à l'intégrité des données ;
- l'enregistrement de données redondantes ou non-concordantes par défaut d'interfaçage ;
- l'obsolescence des équipements, des logiciels, ses solutions métier dédiées..

Les risques juridiques peuvent prendre la forme suivante :

- l'apparition de nouveaux contentieux impliquant les élus ou engageant la responsabilité de la collectivité ;
- la mise en place de contrats ou conventions inadaptées susceptibles de fragiliser les relations partenariales de la collectivité;
- la non prise en compte de certains droits et obligations de la collectivité à défaut d'une veille réglementaire adéquate.

Pour les risques opérationnels, un choix peut être fait des items suivants :

- des dommages sur les bâtiments de la collectivité ou l'espace public ;
- des erreurs et défaillances répétées au détriment des usagers ;
- une dégradation sensible du service rendu.

Du fait de cette profusion de sujets, une collectivité peut se retrouver avec une cartographie contenant plusieurs dizaines - voire même plus d'une centaine - de catégories de risques.

Bien entendu, la gouvernance sera amenée à sélectionner dans ce vaste ensemble un nombre plus restreint de risques faisant l'objet d'un suivi prioritaire, du fait notamment de leur forte criticité, de leur sensibilité politique ou de leur impact particulier sur la réalisation des objectifs du projet de mandat et/ou du projet d'administration subséquent.

→ Voir **Fiche technique 10**

Risques le plus fréquemment rencontrés et exemples d'univers de risques dans différents types de collectivités

Parmi les organismes satellites, on trouve principalement les associations subventionnées, les délégataires de service public, ou toute autre structure dont la collectivité est financeur et/ou représentée dans la gouvernance (présidence, membre d'un comité, …).

Il n'existe pas de définition uniforme des organismes satellites, si bien que chaque collectivité doit être amenée à fixer un certain nombre de critères pour déterminer celles qui parmi ses structures partenaires peuvent effectivement entrer dans cette catégorie.

Au nombre des critères retenus, ceux-ci sont les plus fréquents :

- l'organisme participe à l'exercice des compétences de la collectivité ;
- l'organisme reçoit des subventions de fonctionnement versées par la collectivité ;
- la collectivité participe au capital de l'organisme ;
- des garanties d'emprunt ont été accordées par la collectivité ;
- des élus de la collectivité participent aux instances de gouvernance de l'organisme;
- la collectivité exerce un contrôle sur les activités et/ou les finances de l'organisme.

Ils peuvent être utilisés cumulativement ou alternativement, selon l'appréciation qui en sera faite[59].

Bien entendu, plus la collectivité sera impliquée dans le fonctionnement de l'organisme, plus grands seront les risques auxquels elle sera exposée du fait d'éventuelles dérives de sa part.

Ainsi si l'organisme satellite participe à la délivrance d'un service public opéré par la collectivité, ou délivre en totalité un service public qui lui est confié par la collectivité, celui-ci peut être la source de certains risques et doit donc être associé au périmètre de l'étude.

Quoi qu'il en soit et à titre d'exemple, les risques suivants peuvent être liés aux organismes satellites :

- inadéquation de la nature juridique ;
- non-conformité à la règlementation relative à la mise en concurrence ;
- défaillance d'un organisme satellite ;
- décisions défavorables de l'organisme satellite pour le budget de la collectivité.

Par ailleurs et pour ce qui concerne les risques d'atteinte à la probité, les recommandations de l'Agence Française Anticorruption (AFA) publiées au JORF du 12 janvier 2021 prévoient que « *les organisations qui exercent un contrôle sur d'autres entités s'assurent de la qualité et de l'efficacité du ou des dispositifs anti-corruption déployés dans l'ensemble du périmètre qu'elles contrôlent* »[60].

En conséquence, toute collectivité est en principe tenue de s'assurer de la qualité et de l'efficacité des dispositifs anticorruption mis en place par les organismes placés sous leur contrôle[61] ; tout manquement à cette disposition l'exposerait à un risque de non-conformité.

[59] Il peut être également utile de se référer aux définitions des opérateurs *in house* données par la Cour de justice des communautés européennes (CJCE) notamment dans son arrêt Teckal du 18 novembre 1999 et par le Conseil d'Etat, par exemple dans son arrêt Commune de Marsannay-la-Côte du 6 novembre 2013

[60] Voir les paragraphes 15, 351 et 367 à l'usage des acteurs publics

[61] Sous réserve des contrôles des commissaires aux comptes auprès des associations recevant plus de 153 K€ de financements publics annuellement et dans la mesure où ces contrôles couvrent la correcte application des procédures internes des associations concernées (y compris donc les dispositifs anti-fraude)

Faut-il ajouter les risques liés aux fournisseurs et sous-traitants de la collectivité ?

Comme vu précédemment, la sous-traitance ou la Délégation de service public peut être un moyen de transférer le risque à des tiers[62].

Cependant, les fournisseurs et les sous-traitants participant à la délivrance d'un service public de la collectivité peuvent être la source de risques importants en cas de défaillance de leur part et/ou de conflits quant à l'application des clauses contractuelles ou conventionnelles.

Les risques encourus touchent en dernier lieu à la qualité du service rendu aux usagers, sans préjuger des dommages éventuels pour la collectivité sur le plan juridique et financier.

A ce titre, il paraît pertinent d'intégrer cette question au périmètre de l'étude, soit au travers d'une catégorie de risques distincte, soit en ventilant ces risques entre différents ensembles thématiques par ailleurs constitués[63].

A titre d'exemple, relèvent de cette catégorie les risques suivants :

- capacité insuffisante et non viabilité d'un fournisseur ou d'un sous-traitant ;
- liquidation d'un fournisseur ou d'un sous-traitant.

Faut-il ajouter les risques exogènes dont les leviers d'action sont en dehors de la collectivité ?

Cette question peut notamment se poser dans le cadre de la répartition de l'exercice des compétences entre collectivités territoriales et l'Etat.

Lorsque cela est nécessaire, même si la collectivité n'est pas à la manœuvre, il est important pour elle que ces risques soient pris en compte afin d'en assurer une traçabilité et un suivi en lien avec les organisations responsables de la mise en œuvre des mesures de maîtrise.

A titre d'exemple, les risques exogènes suivants peuvent être pris en considération :

- terrorisme/attentats ;
- catastrophes naturelles ;
- catastrophes technologiques et industrielles ;
- catastrophes sanitaires.

Pour le traitement de ces risques particuliers qui mettent en jeu la continuité du fonctionnement de la collectivité et la permanence des services rendus à la population, il est recommandé de se référer à la Norme ISO 22301-2019 relative à la Sécurité et à la résilience des organisations confrontées à des risques majeurs [64].

[62] Voir supra, Section 1-B - Points préliminaires

[63] Par exemple des risques de défaillances fournisseurs peuvent être répartis entre des risques liés au Système d'information (SI) de la collectivité s'il s'agit seulement de fournisseurs SI, des risques liés à l'intégrité des personnes s'il est question de fournisseurs de produits alimentaires, sanitaires etc… Ce type de segmentation se justifie notamment si des problématiques bien distinctes s'attachent à chaque type de fournisseur.

[64] Voir supra, Section 1-B-1 et Fiche technique n° 5

3 Passer en phase opérationnelle

Dès lors qu'elle a pu vérifier que les conditions étaient remplies pour conduire en son sein un projet structurant de management des risques - telles que décrites dans la section 2-A - et après avoir pris les arbitrages requis quant à la méthodologie employée et au périmètre du chantier à mener - comme présenté dans la section 2-B - la collectivité est en mesure de construire ou reprendre efficacement sa cartographie des risques et d'établir sur ces bases une démarche assurantielle pérenne.

A cet effet, il lui revient de procéder à une analyse des risques dans le périmètre retenu, en retenant une approche itérative et incrémentale qui repose sur l'identification des risques majeurs et doit amener à leur maîtrise effective selon les modalités les mieux appropriées.

Cette démarche est décrite dans les pages qui suivent ; elle se déploie en deux phases :

- une première phase - qui fait l'objet de la section 3-A - correspond à l'identification de l'ensemble des risques auxquels est exposée la collectivité et à l'évaluation de leur criticité - établie en termes d'impacts et de probabilité - préalablement à la mise en place des mesures de maîtrise appropriées, ces risques se présentent comme des risques bruts (ou inhérents) ;
- une seconde phase - décrite dans la section 3-B - a pour objet de décrire et évaluer les risques nets (ou résiduels) correspondant aux mêmes risques mais avec un degré éventuellement corrigé à la baisse après qu'aient été appliquées les mesures de maîtrise jugées nécessaires.

La conduite de ces différentes étapes s'inscrit principalement dans les principes n° 10 à 14 du cadre de référence du COSO ERM 2017.

Cadre de référence du COSO ERM[65]- Principes n° 10 à 14 relatifs à la Performance

10) Identifier les risques

L'organisation identifie les risques qui affectent la réalisation de la stratégie et des objectifs opérationnels.

11) Évaluer la criticité des risques

L'organisation évalue la criticité des risques.

12) Prioriser les risques

L'organisation priorise les risques pour sélectionner les modalités de traitement de ces risques.

13) Mettre en œuvre les modalités de traitement des risques

L'organisation identifie et sélectionne les modalités de traitement des risques.

14) Développer une vision globale du portefeuille de risques

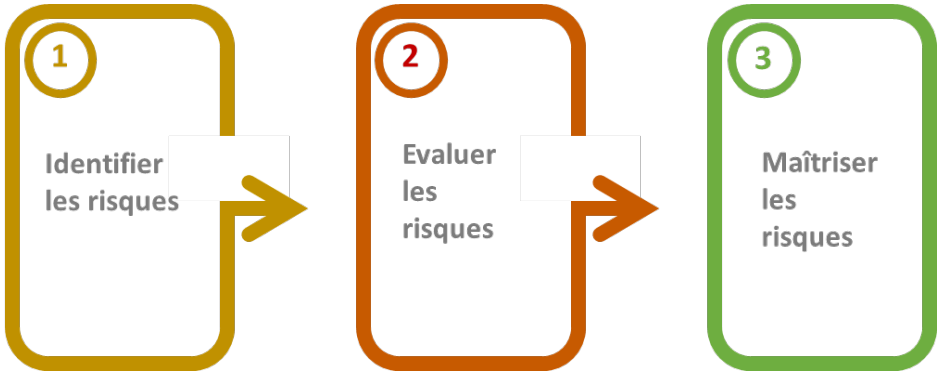
L'organisation développe une vision globale et une évaluation du portefeuille de risques.

[65] COSO ERM - 2017 « Le management des risques de l'entreprise Une démarche intégrée à la stratégie et à la performance »

De l'identification à l'évaluation des risques

Selon différentes normes ou bonnes pratiques en vigueur, une analyse des risques est classiquement organisée en trois étapes principales :

- l'identification des risques ;
- l'évaluation des risques ;
- la maîtrise des risques.



L'identification des risques

Il s'agit dans un premier temps d'identifier les risques ou les situations à risque et leurs causes à partir :

- d'un processus métier et de ses étapes ;
- d'évènements indésirables, dysfonctionnements, difficultés, problèmes, freins, blocages, points de vigilance, vulnérabilités, … avérés ou ressentis ;
- de dangers auxquels l'activité pourrait-être exposée.

L'évaluation et la hiérarchisation des risques

Pour chaque risque identifié, il s'agit ensuite de définir :

- les traitements ou mesures déjà existantes permettant de le réduire ou de le maîtriser ;
- sa vraisemblance, fréquence ou probabilité de survenance ;
- sa gravité (conséquence) s'il vient à se réaliser ;
- sa criticité (degré d'acceptabilité).

La maîtrise des risques

Pour chaque risque identifié, en complément des traitements ou mesures déjà existantes, il s'agit ici d'identifier des mesures complémentaires permettant de les maîtriser :

- des mesures de prévention dont le but sera de diminuer sa probabilité ;
- des mesures de détection et/ou des activités de contrôle ;
- des mesures de protection (ou « mesures curatives ») dont le but sera de diminuer sa gravité.

3-A Etablir le portefeuille des risques de la collectivité

La détermination des risques bruts auxquels est exposée une collectivité résulte directement de l'analyse de ses activités, de ses métiers et de son environnement.

3-A-1 Recenser les risques

Avant de maîtriser ses risques et de s'engager dans une démarche *ad hoc*, il est bien entendu nécessaire de les connaître et de les recenser.

Cette première étape a donc pour objet de procéder à une revue des risques majeurs de la collectivité, en évitant le double écueil d'un inventaire interminable d'événements mineurs ou très particuliers ou on contraire d'une liste sommaire d'événements fourre-tout auxquels il ne serait pas possible d'affecter des causes et des conséquences précises ; dans les deux cas, ces éléments seraient impropres à une politique de pilotage efficace, par manque d'information réellement exploitable.

Réunir les sources utiles et choisir les méthodes d'analyse appropriées

Pour les développements qui suivent, on se bornera à définir un risque étant comme la possibilité que se produise un évènement qui aura un impact défavorable sur la réalisation des objectifs et/ou sur le fonctionnement de la collectivité ; comme vu précédemment, cette approche exclut la prise en compte des éventuelles opportunités qui peuvent être le pendant des menaces identifiées [66].

Par souci d'efficacité, une collectivité peut en effet avoir intérêt à concentrer ses efforts sur le but premier d'une démarche assurantielle qui est de sécuriser sa trajectoire sur le moyen et long terme.

Toutefois elle peut tirer profit de ce travail d'inventaire et d'analyse pour repérer des opportunités latentes et les mettre en pratique afin d'y gagner de nouveaux leviers d'action ; à cet effet, il est de bonne pratique de consigner ces opportunités à mesure que progresse le chantier global, en vue de leur exploitation ultérieure ou même concomitante[67].

Dans ce cadre, différentes sources méthodologiques peuvent être mobilisées pour aider les collectivités à identifier des risques :

- les référentiels métiers ou publications diffusés par des associations professionnelles[68] ou des cabinets spécialisés ;
- les référentiels spécialisés, comme la base de données des dangers, support à la méthode AGR (Analyse globale des risques) ou l'outil EBIOS (Expression des besoins et identification des objectifs de sécurité) pour les systèmes d'information.

[66] Voir supra, Section 2-A-2

[67] Voir la Fiche technique n° 17 - Proposition de Fiche synthétique de suivi & de traitement des risques (Fiche A)

[68] En particulier l'Institut français du contrôle et de l'audit internes (IFACI) et l'Association pour le management des risques et des assurances de l'entreprise (AMRAE)

De récents ouvrages dédiés ces questions permettent en outre d'approfondir tout point particulier à la lumière de l'actualité réglementaire et des tendances qui se font jour[69].

En complément de ces supports méthodologiques et techniques, les collectivités pourront également utiliser avec profit certains des outils proposés dans la norme ISO 31000-2018 relative au management des risques.

Ces outils visent à faciliter la conduite du projet à chacune de ces étapes ; ils permettent en particulier de renforcer la traçabilité des analyses menées et à faciliter leur mise en partage, tant au sein de la collectivité qu'au-dehors de celle-ci.

Chaque collectivité dispose ainsi d'un large choix d'options pour construire le mode opératoire le mieux approprié à son organisation et à ses besoins particuliers.

→ Voir **Fiche technique 11**

Outils & méthodes d'évaluation des risques présentés dans la Norme ISO 31000 relative au management des risques

Un canevas de collecte et d'analyse étant constitué en accord avec les standards existants et sur une base proportionnée aux enjeux de la démarche, les matériaux suivants pourront être utilisés :

- description des différentes étapes des processus métier identifiés ;
- retours d'expériences (incidents, évènements indésirables …) internes ou externes[70];
- contentieux de la collectivité passés ou en cours ;
- benchmarks auprès d'acteurs publics.

Ces éléments doivent être examinés au regard de deux questions complémentaires.

La première est tournée vers le passé ; elle vise à connaître les risques ou évènements déjà survenus dans la collectivité.

La seconde regarde vers l'avenir ; il s'agit d'imaginer avec vraisemblance les risques ou évènements qui pourraient survenir dans la collectivité.

En effet, recenser les évènements qui se sont déjà produits dans la collectivité est une première étape intéressante pour engager le chantier, de façon parlante et pragmatique.

Toutefois, il ne suffit pas de regarder en arrière ; il est tout aussi nécessaire de développer une vision prospective et de supposer ce qui pourrait arriver, non pas comme le fruit d'une simple spéculation mais comme le produit d'une réflexion collective reposant sur les enseignements du passé et les effets attendus de paramètres internes et externes précisément étudiés.

En outre et à compter du moment où une démarche de management des risques sera effectivement mise en place, il est recommandé de développer des Fiches de signalement des incidents associés aux différents risques identifiés de manière à objectiver la mesure de leurs fréquences et impacts respectifs ; à mesure que ces Fiches seront créées et consolidées, la démarche prospective de la collectivité s'en trouvera confortée et les projections faites y gagneront graduellement en crédibilité [71]

[69] Voir la Bibliographie et plus particulièrement la rubrique « Lectures complémentaires recommandées »

[70] Pour le recensement et la collecte des incidents, voir la Fiche technique n° 17 « Exemple de Fiche synthétique de suivi et de traitement d'un risque (criticité & maitrise) » et plus particulièrement le modèle B « Fiche de signalement d'un incident »

[71] Voir la Fiche technique n° 17 - Proposition de Fiche de signalement d'un incident (Fiche B)

L'identification et l'analyse des risques peuvent être réalisées de différentes manières, telles que l'organisation d'ateliers de travail, la réalisation de questionnaires, la tenue d'entretiens individuels.

Les ateliers de travail doivent *a minima* réunir autour d'une table ou d'une caméra :

- un animateur, qui est en général le manager des risques de la collectivité ou le préfigurateur de la démarche pour celles qui sont moins avancées ;
- des opérationnels et experts métiers en fonction du domaine ou périmètre couvert par l'analyse, en ayant le souci de mixer les fonctions et les niveaux de responsabilité.

Pour fluidifier les échanges et faciliter l'émergence de consensus entre les parties engagées, différentes méthodes d'animation de groupes de travail peuvent être utilisées, telles que les techniques de brainstorming ou remue-méninges.

Le brainstorming pour atteindre un consensus entre experts et référents métier

Le brainstorming est une méthode éprouvée et efficace pour créer un consensus entre techniciens et experts sur un sujet d'intérêt commun.

Elle figure d'ailleurs parmi les instruments recommandés dans la Norme ISO 31000 relative au management des risques, parallèlement à d'autres pratiques similaires comme les entretiens structurés ou semi-structurés et la Technique Delphi[72].

Identifier les risques de la collectivité

Afin d'avoir une vue à 360 degrés des principaux risques d'une collectivité du point de vue de ses dirigeants, une collectivité peut engager une démarche de type *top-down* selon une approche par les risques majeurs de la collectivité ; toutefois, elle aura soin de tempérer cette approche dans un sens participatif afin de ne censurer aucune prise de parole et de s'assurer d'une contribution active de l'ensemble des agents concernés à chaque niveau de responsabilité [73].

Sur cette base, il y aura lieu de rechercher les risques majeurs et significatifs auxquels la collectivité est exposée, dans le périmètre d'activité préalablement déterminé ; ces risques pourront notamment être examinés par objectif ou par processus selon l'entrée qui sera retenue [74].

On entend respectivement par risques majeurs et significatifs :

- la possibilité de survenance d'événements qui seraient de nature à compromettre irrémédiablement la réussite du projet de mandat et plus encore qui mettrait la collectivité en situation de ne plus remplir ses missions essentielles ;
- la possibilité de survenance d'événements ayant un impact durable et clairement mesurable sur le fonctionnement de la collectivité et la mise en œuvre des politiques dont elle a la charge.

[72] Voir l'Annexe n° 1 de la Fiche technique n° 11

[73] Voir supra, Section 2-B-2

[74] Voir supra, Section 2-B-1

Ces impacts potentiels doivent être appréciés de manière large, en tenant compte des critères humains (comme un accident grave et invalidant), juridiques (du type d'une condamnation pénale) ou opérationnel (à l'image d'une dégradation sensible voire d'une rupture durable du service rendu au public).

L'étude de ce périmètre présente l'avantage de permettre l'identification - d'abord de manière macroscopique - des risques ou les situations à risque auxquels la collectivité est susceptible d'être confrontée ; ultérieurement ces risques pourront être regroupés afin de faciliter leur pilotage à l'échelle de la collectivité.

Deux questions pourront être posées à cet endroit.

La première question vise à déterminer les risques majeurs pour la collectivité, tous domaines confondus.

Ces risques doivent être en nombre resserré - par exemple, pas plus de cinq - car il s'agit bien du point de référence ultime pour mesurer, en temps utile, la criticité de tous les autres risques retenus.

La seconde question vient subsidiairement et porte sur les risques significatifs pour chacun des domaines de compétence de la collectivité, en tenant compte des fonctions support aussi bien que des fonctions métier dédiées à la mise en œuvre des politiques dont elle a la charge.

Cette recherche doit être étendue jusqu'à couvrir l'ensemble du périmètre de management des risques, tel que défini au démarrage du chantier[75] .

Par une démarche en entonnoir, ce premier panorama permet de cibler les processus susceptibles de présenter des points de fragilité et de mener une analyse en profondeur permettant d'évaluer le degré de vulnérabilité de la collectivité sur chacun d'entre eux.

Documenter et caractériser les risques

Afin de pouvoir apprécier la vraisemblance que des risques déjà observés - ou non - se produisent dans le futur et de mesurer leur incidence potentielle, il convient d'apporter à chacun d'entre eux la documentation suivante :

- causes et/ou facteur déclencheur ;
- détermination de ses conséquences ;
- mesures ou traitements déjà en place pour réduire la possibilité de survenance de l'événement considéré et/ou en atténuer les effets.

A cet égard, quatre questions doivent être systématiquement posées.

La première question touche aux **causes** ou évènements qui ont pu engendrer - ou pourraient engendrer - la situation décrite.

La seconde question a trait à son **impact**, qui représente ses conséquences directes et éventuellement indirectes.

La troisième question concerne sa **probabilité**, soit sa fréquence estimée dans un horizon temporel prédictible.

[75] Voir supra, Section 2-B-3

La quatrième question porte sur les **mesures de maîtrise existantes** pour réduire ou maîtriser cette situation.

Ces points pourront être étudiés et tranchés en mobilisant des experts métiers dans la continuité des ateliers d'identification des risques, sous l'animation du manager des risques ou le cas échéant du préfigurateur de la démarche de management des risques au sein de la collectivité.

Première question - La recherche des causes

Différentes méthodes peuvent contribuent à la recherche des causes et événements déclencheurs d'une situation caractéristique d'un risque.

Ces méthodes sont à l'appréciation des groupes de travail constitués, avec le souci de privilégier les approches participatives permettant une libre circulation des vues et opinions.

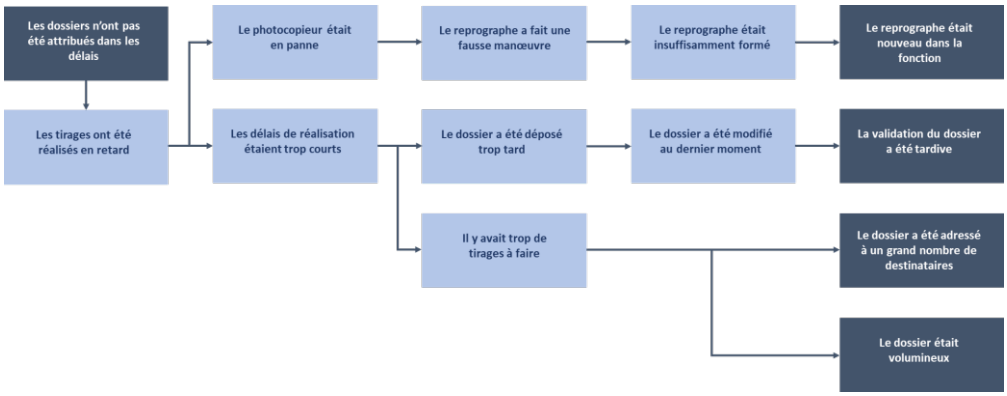
A cet égard, il est recommandé de se référer au vaste panel d'outils et méthodes visant au dépistage des causes, à l'identification des conséquences et à la modélisation des process présent dans la Norme ISO 31000-2018[76].

La méthode des 5P ou « Arbre des causes » pour approfondir la recherche des causes

La méthode des 5P (ou 5 « pourquoi ») consiste, à partir d'un phénomène observé ou potentiel, à poser 5 fois de suite la question « pourquoi » afin d'en identifier les causes racines.

Bien entendu, le nombre de 5 n'est pas une obligation. Il peut en effet être adapté au cas par cas, avec plus ou moins d'itérations en fonction de la complexité ou de la nature du phénomène à analyser.

L'exemple suivant montre comment cette méthode permet d'analyse un événement donné (« Les dossiers n'ont pas été attribués dans les délais ») et d'en extraire quatre causes racines[77].



Cette méthode figure parmi les instruments recommandés dans la Norme ISO 31000 relative au management des risques sous l'appellation « *Analyse de causes profondes* » (référence B-12).

[76] Voir Fiche technique n° 17

[77] Exemple issu du département du Pas-de-Calais

Deuxième question - La mesure de l'impact

De prime abord, il convient de ne s'interdire *a priori* aucune mesure d'impact.

Il n'est en effet pas souhaitable de borner l'exercice aux seuls risques susceptibles d'affecter les intérêts essentiels de la collectivité - tels qu'on peut les comprendre au regard des risques majeurs susmentionnés - car on perdrait alors toute visibilité sur l'évolution de risques mineurs dont l'impact cumulé est susceptible de porter un préjudice significatif et durable au fonctionnement de l'organisation.

Pour la mesure de l'impact, on peut se servir d'une grille créée *ad hoc* qui permettra d'établir et représenter plusieurs niveaux de conséquences - par graduation progressive - pour les différents critères sélectionnés, tel que par exemples l'intégrité des agents, la continuité du service, la réputation de la collectivité…

Cette grille doit être élaborée en lien étroit avec les décideurs et avec le niveau d'appétence au risque précédemment évoqué[78].

De manière générale, l'impact ou la sévérité du risque doivent s'apprécier largement, en retenant des critères humains, financiers, juridiques et réglementaires, opérationnels, voire réputationnels et politiques.

Le nombre de niveaux n'est pas anodin dans le cadre d'une évaluation, car les personnes interrogées ont une tendance à choisir le niveau intermédiaire s'il existe, ce qui peut être contre-productif car tous les risques se retrouveront dans la même zone.

Par exemple, pour le critère de réputation on peut considérer qu'une dépêche ou un *tweet* peu repris sera d'un niveau d'impact minimal (par exemple faible ou limité) alors qu'une crise médiatique à échelle nationale sera considérée comme d'un niveau d'impact maximal (par exemple catastrophique).

De même, pour faciliter l'évaluation de l'impact il est recommandé d'avoir recours à des scenarii illustratifs qui permettent aux personnes participant à l'évaluation de mieux visualiser les causes et conséquences du risque évoqué. Ce ou ces scenarii doivent être poussés à une crédibilité de survenance maximale.

Afin d'agréger ces critères, on peut soit choisir de conserver l'évaluation la plus pessimiste, soit réaliser une moyenne pondérée.

Troisième question - L'évaluation de la probabilité

La probabilité d'un risque correspond à son degré d'occurrence estimé à l'horizon de temps retenu.

Il s'agit donc d'une projection vraisemblable qui repose essentiellement sur :

- l'historique des événements passés ;
- l'analyse de ses causes intrinsèques du risque qui permet d'estimer le degré de rareté des conjonctions nécessaires pour qu'il se produise de nouveau.

Comme pour l'évaluation de l'impact, il est généralement utile de réaliser ce type de simulation en appui de scénarii illustratifs visant à une meilleure appropriation des mécanismes à l'œuvre dans la survenance du risque et des éventuelles circonstances facilitantes.

A cet égard et sauf raison particulière pour procéder autrement, il est recommandé de rechercher la fréquence escomptée de l'événement sur une période correspondant à la durée du mandat.

[78] Voir supra, Section 2-A-2

Quatrième question - L'identification des mesures de maîtrise existantes

Il s'agit à ce point de déterminer les mesures de maîtrise observées précisément au moment où le risque a été reconnu et qualifié.

Ces mesures de maîtrise prennent principalement la forme de contrôles et pointages à la charge des services opérationnels engagés dans la mise en œuvre du processus analysé ainsi que des tâches de supervision revenant au management.

Elles peuvent également se présenter comme des analyses, enquêtes, vérifications réalisées par des fonctions support de la collectivité (contrôle de gestion, service qualité…).

De manière générale, les risques à fort impact sont identifiés et maîtrisés.

En revanche, l'expérience montre qu'un intérêt particulier doit être porté aux risques récurrents mais de faibles impacts, délaissés en matière de contrôle interne mais dont l'impact cumulé peut être en définitif conséquent.

Toutefois, il est important d'inscrire la démarche de maîtrise des risques dans un projet de simplification et de consolidation de l'existant ; à cet égard, la démarche assurantielle doit être conduite dans le souci de valoriser les mesures en place et limiter autant que possible la création de dispositifs additionnels.

L'analyse du risque doit ainsi recenser tous les dispositifs de maîtrise existants, y compris dans le cas où ceux-ci seraient appliqués sans consigne écrite ou sans supervision clairement organisée. En effet, ces contrôles embryonnaires peuvent servir de point d'appui pour développer un système de maîtrise plus abouti, le cas échéant en faisant appel au regard croisé de plusieurs agents non subordonnés l'un à l'autre ou en créant une chaine de reporting et de validation *ad hoc*.

Exemple pour un Département :

Pour un Département, un risque majeur peut être le dysfonctionnement des processus de protection de l'enfance ; la prééminence de ce risque résulte des forts enjeux attachés à la mise en œuvre de ces politiques et aux nombreuses failles possibles dans la conduite de telles actions.

En réponse à la détermination de ce risque majeur il convient d'analyser en profondeur le recueil et le traitement des informations préoccupantes.

Les informations recueillies porteront en premier lieu sur la fréquence et la gravité des incidents signalés sur ce domaine dans un passé relativement récent, une période minimale d'observation de cinq années étant à rechercher dans la mesure du possible.

Au-delà de cette observation, il est nécessaire d'analyser les causes de ces incidents afin de déterminer s'ils sont susceptibles de se reproduire et dans l'affirmative avec quels effets et à quelle périodicité vraisemblable.

L'ensemble de ces éléments permettra de mesurer sur une base objective le degré de vulnérabilité de la collectivité envers ce risque particulier.

L'analyse ainsi menée sera également utile pour identifier les points de contrôle déjà existants et plus généralement pour évaluer le dispositif de maîtrise visant à atténuer la vulnérabilité de la collectivité.

3-A-2 Regrouper les risques

Le processus d'identification et caractérisation des risques majeurs et significatifs de la collectivité conduit d'ordinaire à la désignation de plusieurs centaines de risques.

Or un tel nombre de risques ne se prête pas à un pilotage efficace des menaces prioritaires ; il est bien préférable de limiter par l'expression des risques à un nombre donné qui sera bien sûr dépendant de la taille et des domaines de compétence de la collectivité mais ne devrait en aucun cas dépasser quelques dizaines.

A ce stade du chantier, il est donc recommandé de procéder à un regroupement des risques dans une limite raisonnable qui ne devrait en principe pas dépasser la centaine.

Un tel résultat peut notamment être obtenu de la manière suivante :

- en regroupant tous les risques liés aux personnes dans le cadre de leurs conditions de travail ou pour les lieux ouverts au public ;
- en regroupant les risques pour lesquels les principaux moyens de maîtrise sont externes à la collectivité, par exemple les compétences de l'Etat ou d'autres collectivités, les risques industriels ;
- en regroupant les risques faisant l'objet d'une cartographie spécifique, par exemple les risques d'atteinte à la probité, les risques de sécurité informatique ;
- en distinguant les risques transversaux, qui parce qu'ils concernent un maximum de personnes et de secteurs d'activité différents, voire le public accueilli, ont forcément un impact potentiel important sur le fonctionnement de la collectivité.

Pour faciliter cet exercice, la collectivité pourra tirer parti des possibilités de classification multiple des risques ; ceux-ci peuvent en effet être analysés par nature (juridique, financier, opérationnel…) par origine (interne ou externe), par niveau d'objectif (politique, stratégique, opérationnel) en vue de leur regroupement dans la forme la mieux appropriée aux attentes de la gouvernance.

La réduction à une liste de quelques dizaines de risques par collectivité exige des choix et oblige leurs auteurs à prendre leurs responsabilités, en tant que garants de la qualité et de la fiabilité du contrôle interne au sein de la collectivité, sur la base de leur propre analyse.

Aussi, pour garantir la fiabilité de ces recoupements, il s'avère extrêmement utile de vérifier la liste ainsi établie, à la fois des processus et des risques liés, avec chacun des responsables opérationnels, pour la part qui les concerne.

Possibilité de distinguer un nombre limité de risques faisant l'objet d'un suivi prioritaire

Quand bien même elle se limiterait à ses risques endogènes et au regard des nombreuses catégories proposées, une collectivité peut difficilement comprimer sa cartographie au-delà de quelques dizaines de risques.

Toutefois ce nombre peut faire obstacle à un pilotage efficace du dispositif global.

Ainsi, la gouvernance est fondée à définir dans cet ensemble un nombre resserré de risques qui feront l'objet d'un suivi prioritaire.

Il peut s'agir des risques présentant la plus grande criticité et/ou de risques avec une sensibilité politique particulière ; dans tous les cas, ce choix appartient seulement à la gouvernance et répond à des motifs d'opportunité.

3-A-3 Evaluer et hiérarchiser les risques

A ce point d'avancement des travaux, le nombre de risques compris dans la cartographie de la collectivité est stabilisé et leur périmètre respectif est déterminé.

De même, la collectivité dispose désormais des éléments clés caractérisant chacun d'entre eux, à savoir ses causes, ses conséquences, sa probabilité et les mesures de maîtrise existantes ; ces éléments seront déterminants pour autoriser l'éventuel regroupement de plusieurs risques similaires.

Déterminer la criticité des risques

La combinaison des conséquences, de la probabilité et des moyens de maîtrise d'un risque permet d'établir sa **criticité**, qui est la mesure du degré d'exposition de la collectivité à sa survenance, exprimée en termes de fréquence et d'impact.

La notion de criticité des risques ne résulte pas d'une évaluation mathématique *stricto sensu* mais d'une analyse multicritères - dont certains sont quantitatifs - qui aboutit à une appréciation collective.

Cet exercice doit être conduit en association étroite avec les responsables opérationnels concernés, de manière à obtenir une évaluation la plus fiable possible.

→ Voir **Fiche technique12**

Exemple d'échelles de criticité des risques

Plus généralement, tout risque est caractérisé par plusieurs degrés distincts de criticité.

Il y a d'abord lieu de se référer à la criticité souhaitée par la gouvernance, ou tout du moins à la criticité acceptable au regard de l'appétence au risque de la collectivité.

Même s'il est difficile de solliciter des directives précises à cet endroit, la gouvernance peut aisément donner des consignes sur certaines catégories de risques. A titre d'exemple, pour les risques liés aux actes contraires à la probité et conformément aux recommandations de l'Agence française anti-corruption (AFA), un niveau minimal de criticité peut être systématiquement ciblé.

On peut ensuite faire mention d'une criticité du risque brut - ou criticité initiale - qui mesure sa probabilité de survenance et son impact potentiel sans tenir compte de l'effet des mesures de maîtrise déjà existantes, qu'il s'agisse des **mesures de maîtrise préventives** qui agissent principalement sur sa probabilité ou des **mesures de maîtrise curatives** qui ont pour objet essentiel de limiter son impact.

Ces différentes mesures constituent l'environnement de contrôle du risque au moment de sa caractérisation ; leur prise en compte permet d'établir une criticité nette initiale caractérisée par une probabilité et un impact potentiel au plus équivalents - et en principe inférieurs - aux valeurs attachées au risque brut.

Enfin, si des moyens de maîtrise additionnels sont ultérieurement mis en place, il convient de tenir compte de leur incidence sur la criticité nette initiale du risque et de définir une criticité nette résiduelle nécessairement plus basse, selon l'efficacité attendue des mesures d'atténuation mises en œuvre.

Ces moyens de maîtrise additionnels peuvent notamment être mis en œuvre si la criticité initiale du risque paraît excessive au regard de sa criticité acceptable ou si elle vient à se dégrader du fait de la remontée d'incidents plus graves et/ou plus fréquents que prévu.

Le processus permanent d'ajustement de ces valeurs est le moteur même de la démarche assurantielle de la collectivité.

L'exemple du risque de cybersécurité

Le risque cyber est une réalité de plus en plus prégnante qui doit être traitée avec une attention grandissante.

Ainsi durant le second semestre 2021, 11 collectivités territoriales ou leurs groupements ont subi des attaques majeures ; neuf d'entre elles étaient de type rançongiciel, une autre portait sur la disponibilité et une dernière a été repoussée avant de pouvoir être caractérisée.

Le vol de données, la paralysie partielle ou totale des services numériques ont des impacts opérationnels, juridiques, financiers ou d'image au moins conséquents.

S'il se combine avec divers facteurs aggravants, ce type d'événement peut même conduire à des crises systémiques aux répercussions dévastatrices sur le fonctionnement des collectivités.

Le récent guide édité par l'ANSSI et le CDSE définit ces crises « d'origine cyber » par « *la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou plusieurs actions malveillantes sur ses services et ses outils numériques (cyberattaques de type rançongiciel, déni de service, etc.). Cet événement à fort impact ne saurait être traité par les processus habituels et courants de l'organisation.*

Les crises cyber ont des caractéristiques propres qu'il est important d'appréhender :

- *Une double temporalité, avec des impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs mois ;*
- *Une absence d'unicité de lieu de réalisation, qui sous-entend une potentielle propagation à d'autres organisations en raison de l'interconnexion des SI ;*
- *Une menace s'adaptant aux mesures d'endiguement et de remédiation ;*
- *Une incertitude concernant le périmètre de la compromission ;*
- *Une complexité pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque. »*[79]

En réponse, les collectivités sont ainsi amenées à se doter d'un dispositif global de maîtrise du risque numérique étendu à la gestion de crise cyber.

Cette évolution intègre des préoccupations techniques et des préoccupations plus stratégiques comme le maintien de l'activité des métiers affectés par la crise ; elle prend notamment la forme de plans d'action engagés pour une meilleure protection et défense des systèmes d'information et des services digitaux.

[79] Guide « Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique » publié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le Club des directeurs de sécurité des entreprises (CDSE) - 2021

Faut-il évaluer successivement des risques bruts et des risques nets ?

La cotation initiale des risques sur la base des risques bruts (sans tenir compte des moyens de maîtrise existants à ce moment) ou des risques nets (en intégrant l'incidence de ces moyens de maîtrise) sont deux options également recevables.

La détermination de risques bruts permet de mesurer plus finement l'enjeu attaché à leur survenance éventuelle et d'apprécier en conséquence la proportionnalité des moyens de maitrise déployés en réponse.

Cet exercice nécessite cependant des outils et méthodes d'évaluation avancés qui permettent de calculer *in abstracto* la probabilité et l'impact de chaque risque identifié puis de la corriger en intégrant précisément l'effet des mesures de maîtrise déjà déployées.

En l'absence de tels outils et méthodes, il paraît préférable d'évaluer initialement les risques sur une base nette, donc déduction faite des mesures de maîtrise déjà en place.

L'exercice d'évaluation des risques bruts peut ainsi s'avérer très théorique et coûteux au regard du bénéfice attendu.

Dans tous les cas, la détermination d'un risque cible permet de mesurer l'écart entre la situation présente et la situation attendue ; cet écart justifie la mise en œuvre d'un plan d'action visant à renforcer les moyens de maîtrise existants.

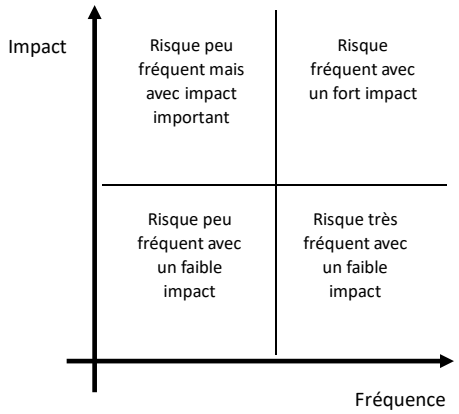
En outre et quelle que soit l'approche retenue, il est important de valoriser les moyens de maîtrise déjà en place lorsqu'ils existent

La criticité des risques comme outil de pilotage d'une démarche assurantielle globale

La détermination de la criticité de chacun des risques inhérents – autrement désignés comme risques bruts ou risques initiaux - de la collectivité résulte de la formule suivante :

Degré d'impact estimé × fréquence présumée dans un avenir prédictible

L'estimation de l'impact et de la fréquence du risque inhérent ne tient pas compte des effets attendus de l'environnement de contrôle observé au moment de son premier enregistrement.



La criticité d'un risque mesuré en termes d'impact et de fréquence permet de créer quatre catégories.

La catégorie des risques fréquents avec un fort impact appelle évidemment en priorité la mise en place des mesures de maîtrise adaptées.

Le risque brut/inhérent est une donnée de référence qu'il convient d'utiliser comme suit.

Evaluation de l'efficacité des mesures de maîtrise existantes

La criticité brute de chaque risque peut être rapportée à sa criticité nette qui tient compte des mesures de maîtrise déjà en place.

La réduction éventuellement apportée à la probabilité et à l'impact présumé du risque permet d'apprécier l'efficacité de ces mesures de maîtrise.

Le cas échéant, mise en œuvre de mesures correctrices dédiées

La criticité brute du risque - ou au besoin sa criticité initiale nette - peut également être rapportée à la criticité souhaitée par la gouvernance, selon son appétence aux risques[80].

Si ces valeurs convergent, il n'y a pas lieu de mettre en œuvre des mesures de maîtrise dédiées.

Ce risque fera toutefois l'objet d'un suivi en continu qui pourra amener à une éventuelle dégradation de sa criticité, notamment dans le cas où sa probabilité et/ou son impact seraient au-delà des projections initiales. De même, le niveau de criticité souhaité par la gouvernance peut être ajusté selon qu'évoluera - ou non - l'appétence au risque de la collectivité.

Dans le cas où la criticité du risque inhérent apparaît d'emblée plus élevée que la criticité souhaitée par la gouvernance, la collectivité sera conduite à déployer des mesures de maîtrise supplémentaires jusqu'à atteindre le niveau attendu.

Au terme de ce processus, il conviendra d'établir un niveau de risques net résiduel selon les modalités décrites dans la section 3-B.

[80] Voir supra - Section 2-A-2

Hiérarchiser les risques

La hiérarchisation des risques constitue la dernière étape du processus.

Elle repose sur la criticité de chacun des risques constitutifs de la cartographie de la collectivité.

Son objet est double :

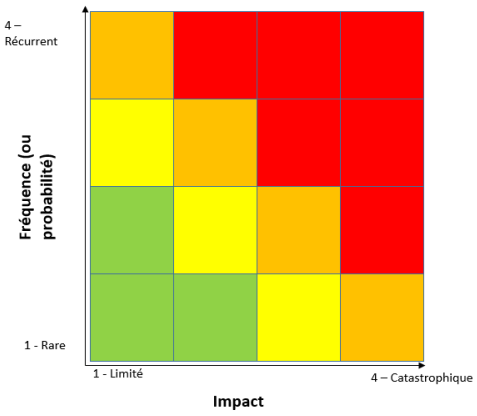
- déterminer les modalités de maîtrise les mieux adaptées à chacun des risques retenus ;
- mesurer le degré global d'exposition de la collectivité et s'assurer qu'il est conforme avec son appétence au risque[81].

Il est recommandé d'utiliser des représentations graphiques pour faciliter cette hiérarchisation.

Ainsi des matrices de criticité représentant les deux axes d'analyse du risque inhérent ou des matrices de priorisation (représentant sur un axe la criticité et sur un autre le niveau de maîtrise) permettent de visualiser graphiquement des groupes de risques en fonction de ces critères.

Ces visualisations sont en outre d'efficaces outils de communication à destination de la gouvernance.

<u>Un mode de représentation traditionnel de la criticité des risques - Le diagramme de Farmer</u>



Le diagramme fréquence-gravité, dit aussi diagramme de Farmer, représente de façon synthétique le risque et les principaux concepts associés.

Il se représente sous la forme d'un cadran à deux dimensions : la fréquence et l'impact. Un point sur le cadre représente un évènement. Avec sa position, une fréquence et une gravité, il représente un risque

Des codes de couleur permettent également d'identifier les zones où sont susceptibles de se retrouver les risques les plus aigus (fréquence et impacts élevés) ou au contraire les zones qui ne donnent pas lieu à des alertes

Ce faisant la collectivité développe une vision globale du portefeuille de risques au sens de la recommandation n° 14 du cadre de référence du COSO-ERM 2017, qui peut être ainsi résumée :

« *La collectivité s'engage à adosser son management des risques à son pilotage stratégique : elle donne à sa gouvernance une vision d'ensemble (exhaustive, transversale, consolidée, évaluable et actualisée) du portefeuille des risques soutenant la répartition des responsabilités et la prise de décision (arbitrage entre niveau d'appétence au risque défini au niveau central et les priorités du mandat)* »[82]

[81] Voir supra, Section 2-A-2

[82] « La Maîtrise des risques dans les collectivités territoriales » - Publication commune de la CIAT et de l'IFACI - 2019

La hiérarchisation des risques permet d'identifier ceux d'entre eux qui exposent la collectivité aux perturbations les plus importantes et durables.

A priori, ces risques ne sont pas acceptables par la gouvernance et doivent être réduits quant à leur probabilité et leur impact présumé par des mesures de maîtrise appropriées.

Ces mesures de maîtrise s'ajoutent aux dispositifs de contrôle et supervision existants, tels qu'observés lors de l'identification et de la caractérisation du risque du ou des risque(s) concerné(s).

Leur mise en place donne lieu à des Plans d'action dont la conduite revient au(x) service métier propriétaire(s) ; dans le cas d'un plan d'action couvrant plusieurs risques rattachés à différents services propriétaires, il peut être opportun de désigner un chef-de-file en charge de la coordination des travaux et de la restitution des résultats obtenus [83].

Détermination de l'acceptabilité des risques

L'acceptabilité d'un risque n'est pas automatiquement liée à sa criticité.

Un risque critique peut ainsi être acceptable tandis qu'un risque mineur serait non-acceptable ; le curseur doit être placé au cas par cas selon le coût de sa maîtrise par la collectivité et les priorités politiques du mandat[84.]

Les décisions prises à cet endroit déterminent le passage éventuel d'une étape d'évaluation à la conduite d'un plan d'action propre à ramener la criticité du risque dans des limites admissibles.

A cet égard, trois façons de procéder peuvent être envisagées :

- conduire un plan d'action pour chaque risque côté au-dessus d'un certain niveau de criticité ;
- se prononcer sur l'acceptabilité de chaque risque et décliner un plan d'actions dès lors que le risque est jugé non acceptable, ceci indépendamment de son degré de criticité ;
- hiérarchiser les risques et décliner un plan d'actions adapté aux différentes catégories créées.

Pour cette dernière méthode, il est de bonne pratique que de combiner la criticité du risque avec d'autres critères comme l'opportunité d'agir, la maturité du contrôle interne, le coût des actions à mettre en œuvre.

Ces solutions alternatives à l'étape clef entre l'évaluation des risques et le déclenchement d'éventuels plans d'action permet d'offrir des possibilités plus variées que le simple classement en fonction du critère de criticité.

Elles sont particulièrement accessibles aux collectivités les plus matures dans leur démarche assurantielle qui disposent d'un panel d'informations suffisant pour assurer un pilotage précis et complet de chacun des risques identifiés.

[83] Voir supra, Section 1-B-2

[84] Voir supra, Section 2-A-2

3-A-4 Etablir un cadre de gouvernance approprié

La criticité des risques constitutifs de la cartographie est un instrument essentiel à la gouvernance du dispositif propre à donner la représentation la plus fidèle possible du degré de vulnérabilité de la collectivité dans son ensemble, en tenant compte de son appétence au risque et des moyens qu'elle est en capacité d'allouer à la maîtrise des principales menaces.

Il s'agit donc d'éléments d'arbitrage essentiels qui doivent être en permanence actualisés et réévalués, dans un processus itératif faisant intervenir les trois lignes de maîtrise des risques.

Leur examen relève du plus haut niveau de gouvernance de la collectivité et ne peut en aucune manière être présenté et réalisé comme une question purement administrative.

A ce point des travaux préparatoires de la démarche, il convient de déterminer les modalités de consultation de l'exécutif, au moyen de rendez-vous réguliers ou préférentiellement dans le cadre du comité des risques[85] créé à cet effet et réuni en présence du maire ou du président de la collectivité ou de son représentant désigné.

Distinguer les rôles et responsabilités respectifs de l'Exécutif et de l'administration

La gouvernance de la collectivité est conjointement assurée par l'exécutif et la direction générale, selon un schéma de partage des responsabilités prévenant toute possibilité de confusion entre les sphères administratives et politiques tout en reconnaissant au maire ou au président de la collectivité un rôle prééminent dans la prise de décision finale.

Les modalités de pilotage et de régulation du dispositif de management des risques répondent aux mêmes exigences.

Les principaux arbitrages relèvent ainsi de l'Exécutif dans la mesure où il est garant de la réalisation des objectifs contenus dans le projet de mandat et du bon fonctionnement de la collectivité[86].

Quant à la Direction générale, il lui revient de mettre en œuvre les arbitrages rendus et d'en faire un reporting exact auprès des élus.

Ainsi, dans la Publication conjointe CIAT-IFACI relative à la mise en œuvre du COSO-ERM 2017 dans les collectivités locales[87], la recommandation n° 1 du cadre de référence du (« *Exercer une surveillance des risques par le conseil* ») est assortie des points d'attention suivants :

« ▪ *Clarifier les responsabilités respectives de chaque acteur.*

- *Être attentif à la place et au rôle de chacun :*
  - *Politique, dans la définition de la stratégie et la validation des priorités pour le mandat en distinguant ce qui relève du conseil et ce qui relève du maire ou du président.*
  - *Administratif, dans la mise en œuvre du plan de maîtrise des risques.*
- *Définir clairement pour le mandat les priorités et les enjeux majeurs en termes de maîtrise des risques.* »

[85] Voir supra, Section1-B-3

[86] De la même façon, la conduite du programme d'audit interne - qui est le dernier maillon de la chaîne de maîtrise des risques - est assurée sous la supervision directe de l'Exécutif - Voir infra, Section 3-B

[87] « Maîtrise des risques dans les collectivités territoriales » - Publication de 2019

3- B- Construire une démarche assurantielle globale

Les dispositifs concourant à la maîtrise des risques visent à obtenir une assurance raisonnable quant à la bonne gestion de la collectivité et à l'atteinte des objectifs attachés au projet de mandat.

Cette assurance se présente comme un instrument de management stratégique et de gouvernance à l'usage de la Direction générale et de l'Exécutif.

En effet, il ne suffit pas pour une collectivité d'identifier les principaux risques attachés à son fonctionnement et à la mise en œuvre des politiques dont elle a la charge ; il lui faut ensuite s'assurer du déploiement de mesures de maîtrise propres à contenir la criticité de ces risques, en proportion avec les moyens dont elle peut disposer et au regard des priorités qu'elle s'est fixées.

Enfin, il revient à la Direction générale de mettre en œuvre une fonction de contrôle interne suffisante pour vérifier en continu le bon fonctionnement du dispositif et la correcte allocation des différentes mesures de maîtrise.

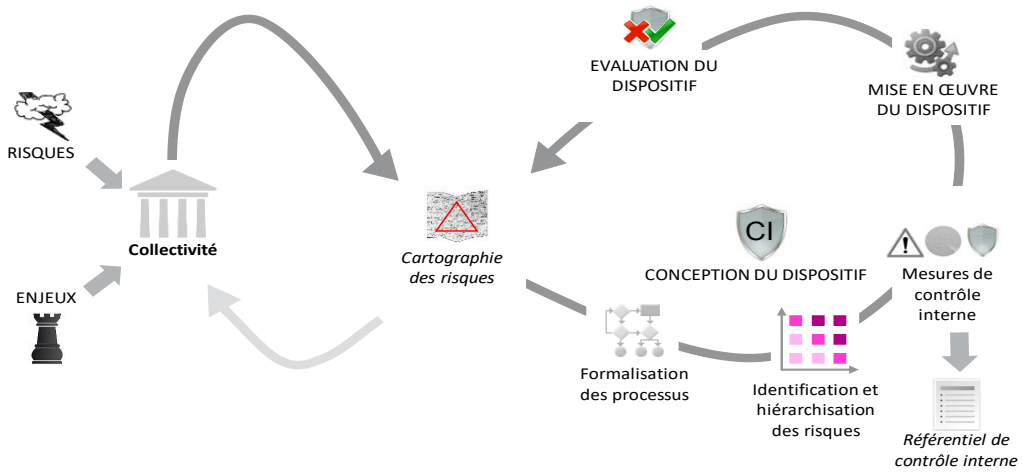
Ce faisant, elle peut délivrer un degré de confiance maximal auprès de l'ensemble des acteurs internes et externes ayant part à la conduite de ses missions.

A cet égard, l'exercice d'élaboration et d'actualisation de la cartographie des risques constitue le fil rouge qui permet d'avancer progressivement vers un objectif de performance globale et de sécurisation de la trajectoire de la collectivité.

Les informations qui en résultent constituent ainsi les éléments indispensables d'une analyse prospective des menaces et opportunités liées à la stratégie de la collectivité et aux évolutions de son environnement, en particulier au regard des points suivants :

- le caractère de systématicité de la revue des risques permet d'attester que les risques prioritaires identifiés sont bien ceux dont la survenance serait la plus à même de compromettre ses intérêts essentiels ;
- l'évaluation des mesures de maîtrise prises en réponse aux risques identifiés permet d'apprécier avec précision son degré d'exposition et de rapporter leur coût aux avantages attendus.

<u>Cartographie des risques dans un processus de management stratégique et assurantiel</u>



Trois points doivent être examinés et arbitrés préalablement à la complète mise en œuvre d'une démarche de maîtrise des risques.

En premier lieu, il importe que la collectivité établisse une méthode simple et robuste pour mesurer séparément la criticité des risques, d'une part sans déploiement des mesures de maîtrise retenues, d'autre part en tenant compte de leurs effets.

En second lieu, si elle fait le choix d'évaluer distinctement le niveau de maîtrise du risque, la collectivité doit se déterminer pour une échelle de notation appropriée.

En troisième et dernier lieu, la collectivité est appelée à se doter d'une instance de pilotage et de suivi donnant toutes les garanties attendues en termes d'expertise et d'indépendance.

Passer des risques bruts aux risques nets

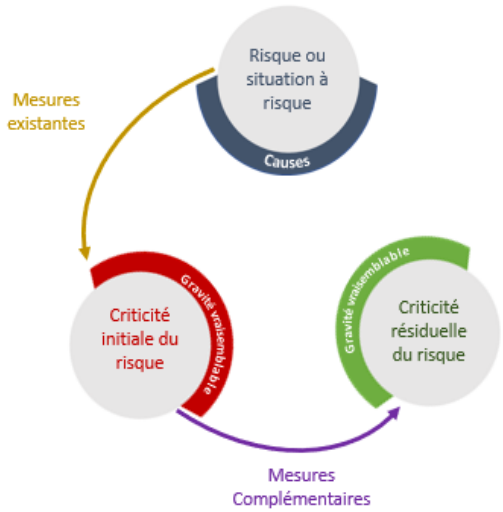
Toute collectivité engagée dans une entreprise d'identification des risques liés à son fonctionnement et à la mise en œuvre des politiques dont elle a la charge est conduite par le besoin d'atténuer la probabilité et l'impact des risques les plus critiques au moyen de mesures préventives et/ou correctives appropriées.

A chaque risque identifié est ainsi attaché un niveau de maîtrise spécifique.

Le niveau de maîtrise correspond au degré d'efficacité des mesures préventives et/ou correctives prises pour contenir le degré de criticité d'un risque - mesuré en termes de probabilité et d'impact - dans des limites que la collectivité juge compatibles avec sa capacité de résilience, les moyens dédiés dont elle peut disposer et la réalisation des objectifs du mandat.

Sur cette base, il est possible d'identifier et évaluer un risque net de l'une ou l'autre des deux manières suivantes :

- une simple réévaluation des niveaux de probabilité et d'impact du risque brut ;
- le maintien des niveaux de probabilité et d'impact du risque brut avec ajout d'un niveau de maîtrise qui permet de mesurer distinctement le degré de mitigation recherché.



Chaîne de traitement du risque

Quelle modalité retenir pour l'évaluation des risques nets ?

Une collectivité peut décider d'ajuster directement le degré de criticité du risque brut sans ajout d'une variable spécifique (option 1) ou maintenir le degré de criticité du risque brut avec une variable additionnelle correspondant au degré de maîtrise (option 2).

Dans la première option, le constat de l'absence de mesure de maîtrise prise en réponse à un risque identifié se traduit par une égale valeur de sa criticité en tant que risque brut et en tant que risque net.

Il s'agit donc d'un système d'évaluation pour partie binaire - qui permet d'identifier aisément les risques non traités - et pour partie quantitatif puisque l'écart entre la criticité brute et la criticité nette du risque constitue un indicateur élémentaire et fiable de la performance des mesures de maitrise mises en œuvre.

Ce mode de représentation pourrait notamment convenir à une collectivité focalisée sur le management des risques à des fins de pilotage stratégique et qui rechercherait prioritairement à connaître les secteurs et politiques les plus exposés, en l'état présent de son organisation.

Dans la seconde option, la mise en place d'un barème de notation du niveau de maîtrise permet de mesurer indépendamment et précisément l'efficience des mesures afférentes, en appui des référentiels en usage pour le contrôle interne et l'audit interne.

Il paraît particulièrement indiqué pour une collectivité qui envisage de développer une fonction de contrôle interne et éventuellement d'audit interne en vue d'un pilotage fin du niveau d'assurance donné au titre de sa bonne gestion et de la réalisation de ses objectifs stratégiques.

Bien entendu, une même collectivité peut évoluer de l'option 1 vers l'option 2 à mesure qu'elle avance dans un processus de connaissance et maîtrise des risques inhérents à son activité.

Toutefois pour alimenter les outils nécessaires au pilotage fin d'une démarche assurantielle globale - et notamment pour établir le tableau MARCI décrit dans la section 3-B-1 - il est recommandé de retenir préférentiellement une évaluation distincte du niveau de maîtrise (option 2) qui permet une mesure plus précise de ce facteur et facilite les interactions entre les différentes parties engagées.

Choisir une échelle de mesure appropriée

Dès lors qu'une collectivité a fait le choix de mesurer chaque risque net au moyen d'une valeur représentant le niveau de maîtrise distincte des éléments de criticité, il lui revient d'établir une échelle où seront décrites les différentes situations susceptibles d'être rencontrées, depuis un système erratique et dépourvu de tout formalisme jusqu'à un système parfaitement documenté, remplissant les critères de performance requis et capable d'apprentissage.

Pour un même risque, l'échelle permettant d'évaluer son degré de maîtrise peut être différente du barème de gradation retenu pour mesurer son niveau de criticité ; il est ainsi tout à fait acceptable de quantifier la maîtrise d'un risque sur une échelle de 1 à 6 tandis que sa criticité se voit attribuer une note comprise entre 1 et 4.

Toutefois, il est conseillé d'utiliser une seule fourchette de valeurs afin de pouvoir rapporter plus aisément les moyens mobilisés au titre des mesures de maîtrise à l'enjeu pour la collectivité, appréciée en termes criticité du risque.

→ Voir **Fiche technique 13**

Proposition pour la mise en place d'une échelle de maîtrise des risques

Mettre en place une instance de pilotage indépendante

Les collectivités dotées d'une troisième ligne de maîtrise des risques ont généralement créé un Comité d'audit en charge de la programmation et du pilotage des travaux d'audit ainsi que du suivi des recommandations formulées à l'issue de précédentes missions.

Bien qu'elle ne revête pas un caractère d'obligation, la création d'un comité d'audit s'inscrit dans les prescriptions de bonne gouvernance associées au déploiement du référentiel COSO, retranscrit et adapté en 2006 par la directive sur le contrôle légal des comptes dans l'Union européenne[88].

Le comité d'audit ne se confond pas avec le comité des risques déjà évoqué à la Section 1-B-3, cependant ces deux instances sont étroitement liées, au moins à un double titre :

- pour la programmation des travaux d'audit, le comité d'audit prend appui sur la cartographie des risques préparée et validée par le comité des risques ;
- le comité des risques tient compte des éventuels ajustements des niveaux de maîtrise des risques compris dans le périmètre de travaux d'audit et/ou de contrôle interne clôturés pour ajuster et actualiser de manière régulière la cartographie des risques.

Ainsi et considérant le fait que le comité d'audit et le comité des risques réunissent sensiblement les mêmes personnes, certaines collectivités ont pu faire le choix d'un comité unique (de type Comité de l'audit et des risques) avec deux formations séparées siégeant distinctement.

Conformément aux prescriptions du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP) le Comité d'audit agit par délégation du maire ou du président de la collectivité ; il convient ainsi qu'il lui rende compte directement de ses résolutions ou tout du moins qu'il les rapporte à un représentant de l'Exécutif désigné à cet effet[89].

De même, le comité d'audit est souvent ouvert à des personnalités extérieures qualifiées qui peuvent apporter un regard expert propre à susciter de nouvelles avancées pratiques et méthodologiques.

[88] Voir l'article 41 de la directive 2006/43/CE du Parlement européen et du conseil du 17 mai 2006 relative au contrôle légal des comptes annuels et des comptes consolidés (dite « huitième directive »)

[89] L'Exécutif exerce les responsabilités au « Conseil » au sens du CRIPP et doit avoir communication de l'ensemble des informations qui y sont mentionnées.

Principales missions d'un comité d'audit

De manière générale, un Comité d'audit est chargé des trois types de missions suivants.

1) Examen et approbation du programme d'audit

Le Comité d'audit prend connaissance de la cartographie des risques de la collectivité dans sa dernière version actualisée[90].

Au vu des éléments présentés, le Comité d'audit :

- sélectionne les travaux constitutifs du programme d'audit - qu'il s'agisse d'audits assurantiels, d'audits conseils ou d'audits de conformité - et alloue à chacun d'entre eux les ressources nécessaires à sa bonne fin ;
- émet un avis sur l'allocation des moyens de la première et seconde ligne de maîtrise des risques et fait toute proposition pour améliorer l'efficience du dispositif existant ;
- examine et approuve le Programme d'audit (annuel ou pluriannuel).

2) Suivi des recommandations faites à l'issue de précédents travaux

Le Comité d'audit est informé de l'avancement des différents plans d'action faisant suite aux recommandations des travaux clôturés.

S'il apparaît que la direction métier s'est abstenue de mettre en œuvre les mesures correctrices attendues sans justification recevable, le Comité d'audit propose des mesures appropriées pour mettre fin à ce dysfonctionnement et diligente d'éventuelles enquêtes complémentaires.

3) Suivi de la démarche d'assurance qualité de la fonction d'audit

Le Comité d'audit approuve l'ensemble des référentiels fixant les règles et procédures de l'audit interne sur le fondement de l'article 2040 du Cadre de référence international des pratiques professionnelles de l'audit interne et toute mise à jour de leur contenu.

Il est également chargé de l'approbation et du suivi du Programme d'assurance et d'amélioration qualité de la fonction d'audit interne[91].

A ce titre il assure le suivi de l'avancement du Programme via l'examen d'un rapport annuel.

En outre, il est informé des modalités de réalisation des évaluations internes et externes de la fonction d'audit[92]

Enfin et le cas échéant, le Comité d'audit émet un avis sur les modalités d'exercice par le Responsable de l'audit interne de missions connexes aux travaux d'audit[93].

[90] Il est entendu ici que le pilotage et le suivi des risques relèvent d'un comité des risques distinct - Voir sa présentation dans la Section 1-B-3

[91] Voir la Norme n° 1300 du Cadre de référence international des pratiques professionnelles de l'audit interne

[92] Voir respectivement les Normes n° 1311 et n° 1312 du Cadre de référence international des pratiques professionnelles de l'audit interne

[93] Voir la Norme n° 1112 du Cadre de référence international des pratiques professionnelles de l'audit interne

3-B-1 Les outils et ressources nécessaires

Dès lors qu'une collectivité, dispose d'une cartographie de l'ensemble de ses risques nets, elle est en situation de mesurer précisément son degré de vulnérabilité face à leur éventuelle survenance et peut mesurer à partir de critères objectifs le bien-fondé des mesures de maîtrise propres à contenir cette menace.

En outre, il lui revient de s'assurer de l'efficience et de la robustesse de ces moyens de maîtrise au moyen d'analyses et de tests appropriés, réalisés sur les points de vulnérabilité reconnus ou présumés.

A cet effet, une fonction de contrôle interne doit être créée et maintenue dans la durée, en appui de moyens internes ou *via* une solution d'externalisation.

En complément, la fonction d'audit interne est exclusivement chargée de la troisième ligne de maîtrise de la collectivité, telle que décrite plus haut[94].

Elle mène à bien cette mission en interaction étroite avec les acteurs en charge de la première et de la seconde ligne de maîtrise.

Il importe que leurs rôles soient précisément définis, en prenant appui sur les référentiels faisant autorité dans les domaines considérés.

Enfin, les droits de chacun des intervenants dans le processus de détermination et ajustement du niveau de maîtrise de chaque risque doivent être clairement établis et hiérarchisés, en cohérence avec la logique interne du dispositif existant.

Principes généraux

Il convient d'abord de considérer le caractère volontariste de la démarche et le fort besoin de transversalité qui la sous-tend.

De ce fait, une construction progressive étalée sur plusieurs mois voire même quelques années peut être un gage de pérennité de la démarche qui doit être considérée comme une option prudente et viable.

Cependant, la cible visée doit dans tous les cas correspondre à des standards reconnus à l'échelle internationale, à défaut de quoi la collectivité ne pourrait être considérée comme dotée d'une troisième ligne de maîtrise des risques, en particulier par des auditeurs externes.

La mise en place d'une fonction d'audit interne au sein d'une collectivité doit ainsi s'inscrire dans un cadre opérationnel et organisationnel garantissant le professionnalisme, l'indépendance et l'objectivité des travaux conduits.

[94] Voir supra – Section 1-B-2

A cet effet, il convient de prendre appui sur les normes issues du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP).

→ Voir **Fiche technique 14**

Normes professionnelles de l'audit interne

Conformément à ces normes, les agents en charge de la fonction d'audit interne ne peuvent prendre directement part à la mise en œuvre des mesures de traitement des risques et ne doivent en aucune manière s'immiscer dans le processus de management des risques car ce faisant ils compromettraient leur indépendance de jugement et se trouveraient dans une situation de juge et partie qui aurait pour effet d'invalider les conclusions de leurs travaux.

En revanche, le responsable de l'audit interne - et plus largement son équipe - sont fondés à superviser le management des risques et donner une assurance quant à la qualité de l'évaluation des risques du point de vue de sa pertinence méthodologique et de son efficacité réelle.

→ Voir **Fiche technique 15**

Rôle de l'audit interne dans le management des risques

Le déploiement d'une fonction d'audit doit ainsi se dérouler en plusieurs étapes correspondant aux phases de mise en place d'un pôle d'expertise avec un accès non restreint à l'ensemble des informations touchant le fonctionnement de la collectivité et la mise en œuvre des politiques dont elle a la charge mais aussi suffisamment éloigné de la chaîne hiérarchique pour investiguer et évaluer toute question à sa convenance sans possibilité de sanction ou de pression de quelque autre nature que ce soit.

Sur ce point, il convient que le responsable de l'audit interne ait un accès direct à l'exécutif et puisse lui rendre compte de toute difficulté dans la conduite de ses missions.

De manière plus large, il appartient à l'exécutif de décider en dernier ressort du contenu ainsi que du calendrier de réalisation du programme d'audit, dans la mesure du possible dans une perspective pluriannuelle.

Pour ce faire, il est appelé à prendre appui sur la cartographie des risques de la collectivité et sélectionner préférentiellement des thèmes d'audit couvrant les risques les plus pertinents pour établir une assurance raisonnable quant à la bonne gestion de la collectivité et sa capacité à atteindre ses objectifs stratégiques et opérationnels.

Dans le cadre de référence de la fonction d'audit il est explicitement prévu que l'ensemble des travaux afférents reposent sur une analyse des risques de l'organisation concernée.

Ainsi la Norme 2010 du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP) relative à la Planification des missions d'audit prévoit que le responsable de l'audit interne établit « *un plan d'audit fondé sur une approche par les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation* ».

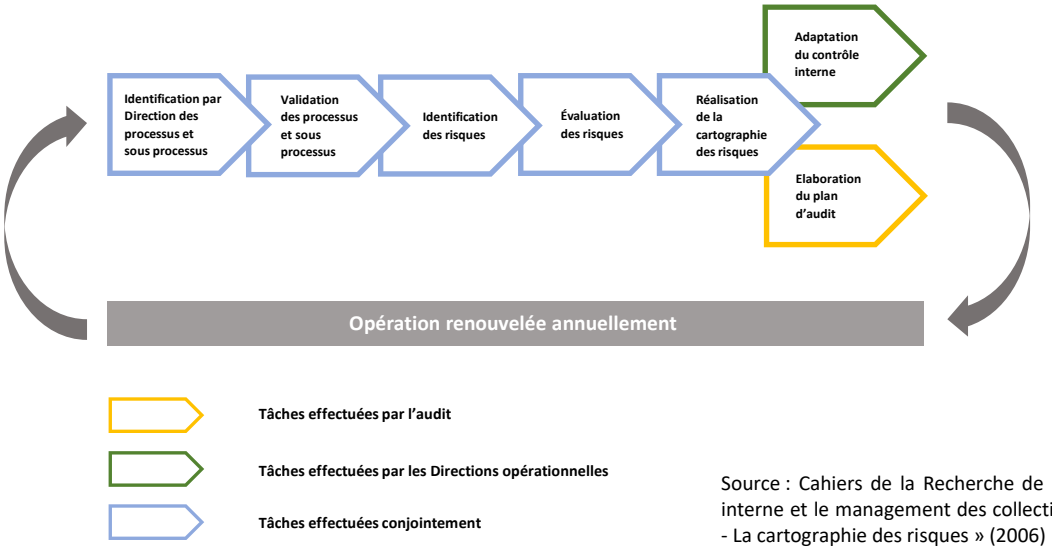
Le responsable de l'audit interne a ainsi vocation à travailler en collaboration étroite avec le manager des risques en vue de la mise en œuvre d'un mécanisme de régulation fondé sur une évaluation continue des zones de vulnérabilité reconnues ou supposées de la collectivité et la mise en œuvre des mesures correctives propres à réparer les faiblesses constatées.

Ce mécanisme itératif repose sur un flux d'échanges permanent entre des acteurs œuvrant de manière autonome dans leurs champs de responsabilité respectifs ; pour que ces échanges soient efficacement et durablement conduits, il importe qu'ils suivent un fil rouge solide et cohérent sous la forme d'un outil partagé tel que la cartographie des risques.

Comme indiqué précédemment, le responsable de l'audit interne est appelé à participer au déploiement de la cartographie des risques de la collectivité en tant que garant de l'approche méthodologique retenue et de sa mise en œuvre pleine et entière ; il s'abstient toutefois de prendre part à tout choix susceptible d'affecter l'objectivité et l'indépendance de ses analyses futures.

En retour, il utilise les informations issues de la cartographie des risques pour orienter le programme d'audit et identifier le périmètre des missions les mieux à même d'étayer une opinion documentée et objective sur la qualité de gestion de la collectivité et la vraisemblance de l'atteinte effective des objectifs du projet de mandat.

Interactions entre le management des risques et la mise en œuvre de programmes d'audit interne



Source : Cahiers de la Recherche de l'IFACI - « L'audit interne et le management des collectivités territoriales - La cartographie des risques » (2006)

A cet égard, il est recommandé que la collectivité mette en place un outil décisionnel permettant de positionner l'ensemble des risques - ou tout du moins les risques majeurs - sur une échelle d'évaluation distinguant leur degré de criticité et leur niveau de maîtrise.

Cet outil doit ainsi permettre de classifier les risques en quatre catégories :

- Les risques à fort degré de criticité et à fort niveau de maîtrise ;
- Les risques à fort degré de criticité et à faible niveau de maîtrise ;
- Les risques à faible degré de criticité et à fort niveau de maîtrise ;
- Les risques à faible degré de criticité et à faible niveau de maîtrise.

Le partage des risques étant effectué conformément à cette grille de lecture, une base d'analyse solide est disponible pour le choix des travaux d'audit à venir.

i. Cas des risques à forte criticité et à fort degré de maîtrise

De manière générale, les travaux d'audit doivent porter en priorité sur des domaines ou des processus couvrant des risques à forte criticité et fort degré de maîtrise présumé.

L'objet de ces travaux d'audit et précisément de tester - ou challenger - le niveau de maîtrise attaché au(x) risque(s) concerné(s) afin de vérifier le bien-fondé de la note élevée attribuée par la direction métier concernée, ou éventuellement en dernier lieu le responsable du contrôle interne.

En pareil cas, la mission d'audit peut aboutir à l'une ou l'autre des conclusions suivantes :

- Maintien de la note attribuée, sans qu'il y ait besoin pour la direction métier d'apporter d'éventuelles mesures correctrices ;
- Maintien de la note attribuée conditionné à la conduite d'un plan d'action contenant les mesures propres à renforcer la maîtrise des risques considérés, à charge pour le responsable de l'audit interne de réitérer ses réserves s'il constate que le plan d'action n'a pas été entièrement mené à bien dans les délais convenus ;
- Mise en question immédiate de la note de maîtrise, la direction métier étant invitée à mener à bien un plan d'action pour rétablir le niveau préalablement affiché ou même pour le réévaluer dans une approche globale de sécurisation des processus de gestion et de contrôle de la collectivité.

Les travaux ainsi menés s'inscrivent dans une mission d'assurance visant à vérifier la robustesse et l'efficience des moyens de maîtrise des principaux risques identifiés.

ii. Cas des risques à forte criticité et à faible degré de maîtrise

En second lieu, certains travaux d'audit peuvent concerner les domaines ou des processus couvrant des risques à forte criticité et faible degré de maîtrise.

Dans cette hypothèse, leur objet n'est pas tant de tester les mesures de maîtrise existantes - puisqu'il est connu par avance qu'elles sont faibles - mais bien plutôt de formuler des recommandations en vue de leur renforcement à moyen et long terme.

Les suites à donner à ces recommandations sont laissées à l'appréciation de l'exécutif et de la direction générale ; ils peuvent ainsi sciemment choisir de maintenir un niveau d'exposition élevé selon leur appétence aux risques et au regard de considérations en opportunité guidées par les circonstances et le contexte général de la collectivité.

Les audits ainsi conduits prennent la forme de missions de conseil visant à proposer des voies et un calendrier pour améliorer des mesures de maîtrise reconnues comme lacunaires.

iii. Cas des risques à faible criticité

Enfin il n'y a en principe pas lieu de mener des travaux d'audit dans les domaines ou les processus couvrant des risques à faible criticité.

Toutefois, la Direction générale doit être amenée à porter une attention particulière aux risques présentés comme étant à faible degré de criticité et à fort niveau de maîtrise.

En effet, pour ces risques particuliers, il y a lieu de s'interroger sur l'opportunité qu'il y aurait à maintenir des moyens de maîtrise importants au regard du peu d'enjeu attaché à la survenance de l'événement considéré.

Dans ce cas, il peut être opportun de réduire les moyens de maîtrise existants, quitte éventuellement à les réallouer à des risques reconnus comme étant à forte criticité

Cet exercice permet de vérifier le respect d'un principe de proportionnalité entre les moyens mobilisés et l'objectif poursuivi ; il s'inscrit également dans un objectif d'optimisation des ressources humaines et matérielles de la collectivité.

En dernier lieu, la Direction générale est appelée à un devoir de vigilance sur l'évolution des risques affichés comme étant à faible degré de criticité et à faible niveau de maîtrise.

Ces risques n'ont pas vocation à être un sujet d'inquiétude particulier pour la collectivité, en dehors du cas où le cumul de leurs impacts respectifs conduirait à des dommages importants propres à faire obstacle au fonctionnement et/ou à la mise en œuvre des politiques de la collectivité.

Dans cette hypothèse, la Direction générale sera conduite à les requalifier de risques à fort degré de criticité et à faible niveau de maîtrise avant de les traiter en conséquence (voir supra).

→ Voir **Fiche technique 16**

Le tableau MARCI comme outil de pilotage des audits

3-B-2 Piloter et optimiser les mesures de maîtrise

Le basculement de l'ensemble des risques de la collectivité en risques nets permet de déployer un dispositif de pilotage des mesures de maîtrise prises sur la totalité des points de vulnérabilité repérés.

La mise en place de ce dispositif de pilotage constitue la condition préalable à l'obtention d'une assurance raisonnable quant à la bonne gestion de la collectivité et à l'atteinte de ses objectifs stratégiques et opérationnels.

Il prend la forme d'un processus dynamique d'interactions entre les acteurs en charge des différentes lignes de maîtrise des risques qui doit permettre d'atteindre un équilibre entre le degré de protection dont dispose la collectivité et les moyens de contrôle et supervisions qu'elle est en situation de mobiliser à cet effet.

Il appartient à la direction générale et à l'exécutif de s'assurer en permanence que la collectivité se trouve dans cette zone d'équilibre au travers d'un réexamen régulier de la criticité des risques auxquels celle-ci est exposée et de l'efficacité des moyens de maîtrise correspondants, telle que vérifiée par le contrôle interne et le cas échéant des travaux d'audit additionnels.

Processus de détermination et d'ajustement du niveau de maîtrise des risques

Un mécanisme de fixation et de réglage en continu du niveau de maîtrise des risques de la collectivité doit être mis en place afin de pouvoir donner à l'exécutif et à la direction générale une image en permanence exacte de son degré d'exposition aux différentes menaces identifiées.

Pour sa parfaite lisibilité, ce mécanisme doit être modelé sur le système des trois lignes de maîtrise des risques recommandé par l'IIA (*Institute of internal auditors*) et précédemment exposé[95].

La direction métier est juge en premier ressort du niveau de maîtrise des risques

L'évaluation de la robustesse et de l'efficience des mesures de maîtrise de chaque risque revient en premier au lieu à la direction métier désignée comme propriétaire.

Cette évaluation est d'abord réalisée concomitamment à l'identification du risque ; elle peut également s'appuyer sur les résultats de travaux de contrôle interne.

Dès ce moment et dans la mesure où la direction métier estimerait que le niveau de maîtrise du risque est insuffisant, elle peut de sa propre initiative conduire un plan d'actions visant à la correction des insuffisances constatées et à une réévaluation globale des mesures existantes.

Ce plan d'actions doit être assorti d'un calendrier de réalisation et d'indicateurs permettant de vérifier l'atteinte des objectifs fixés ; il doit également cibler un niveau de maîtrise plus élevé qui pourra être validé à compter de la complète exécution des engagements y afférents.

[95] Voir plus haut - Section I-B-2

Modalités d'ajustement éventuel du niveau de maîtrise établi par la direction métier

L'établissement du degré de maîtrise d'un risque relève de la responsabilité de la direction métier propriétaire.

Cette opération n'est toutefois en aucun cas le fruit d'une appréciation solitaire.

En effet, le niveau de maîtrise d'un risque a vocation à être évalué en continu dans le cadre des dispositifs de contrôle interne et éventuellement consolidé *via* des plans d'action ciblés.

De surcroît, ce même niveau de maîtrise peut à tout moment être challengé par les auditeurs internes en charge de la troisième ligne de maîtrise ainsi que par tout auditeur externe habilité.

Pour autant, il n'appartient pas davantage au responsable de l'audit interne - ou à un responsable de la fonction contrôle interne - d'utiliser les conclusions de ces travaux pour corriger unilatéralement le niveau de maîtrise du ou des risque(s) concerné(s).

Dans le cas où les investigations menées ont mis en évidence des dysfonctionnements significatifs des mesures de maîtrise existantes, le responsable de l'audit interne ou le référent contrôle interne ont seulement la possibilité de formuler des alertes quant à l'inexactitude de leur niveau de maîtrise présumé et de recommander la mise en place de mesures correctrices appropriées.

En réponse, la direction métier propriétaire est appelée à mener à bien un plan d'action constitué des mesures correctrices attendues.

A compter de sa complète réalisation, les réserves (ou alertes) posées par le responsable de l'audit interne ou le responsable du contrôle interne pourront être levées, ce qui aura pour effet de consolider le niveau de maîtrise initial du ou des risque(s) couvert(s).

Toutefois, si la direction métier propriétaire s'abstient de mettre en œuvre le plan d'action demandé dans les délais prescrits, il revient au manager des risques de réévaluer en conséquence le niveau de maîtrise du ou des risque(s) en cause.

Cet ajustement doit être opéré à l'issue d'un dialogue ouvert et transparent avec la direction métier propriétaire et le responsable de l'audit interne - ou le référent contrôle interne à l'origine des réserves (ou alertes) formulées.

En cas de désaccord entre eux, il appartient à la gouvernance de trancher et d'établir le niveau de maîtrise du ou des risque(s) contesté(s).

Il s'ensuit que la détermination du niveau de maîtrise des risques de la collectivité est une question relevant de l'arbitrage final de la gouvernance, sous la double réserve suivante :

- cet arbitrage est éclairé par les travaux de contrôle et audit les plus récents ;
- un processus itératif permanent doit être établi et entretenu par le manager des risques pour obtenir autant que possible des positions partagées entre les différentes lignes de maîtrise impliquées.

Bien entendu, de nouveaux audits ou contrôles pourront intervenir ultérieurement et, le cas échéant, mettre de nouveau en cause l'efficacité des mesures de maîtrise en place ; un tel constat conduirait à la formulation de recommandations additionnelles et continuerait le cycle jusqu'à ce que puisse être établie la parfaite fiabilité des dispositifs prévus et reconnus nécessaires.

Exemple d'itération pour l'évaluation du degré de maîtrise d'un risque

A un **temps T**, un risque déterminé se voit attribuer par le service métier propriétaire un degré de maîtrise 4 (« Supervisé ») au regard du dispositif de contrôle de premier niveau établi en réponse.

A **T + 3 mois**, le responsable du contrôle interne procède à une analyse du dispositif de contrôle de premier niveau accompagnée de tests ; cet exercice met en évidence certains dysfonctionnements qui conduisent à des réserves sur la note attribuée.

En réponse, le service métier propriétaire du risque mène à bien un plan d'action qui a pour objet de corriger les dysfonctionnements constatés par le responsable du contrôle interne et de renforcer plus globalement les procédures existantes.

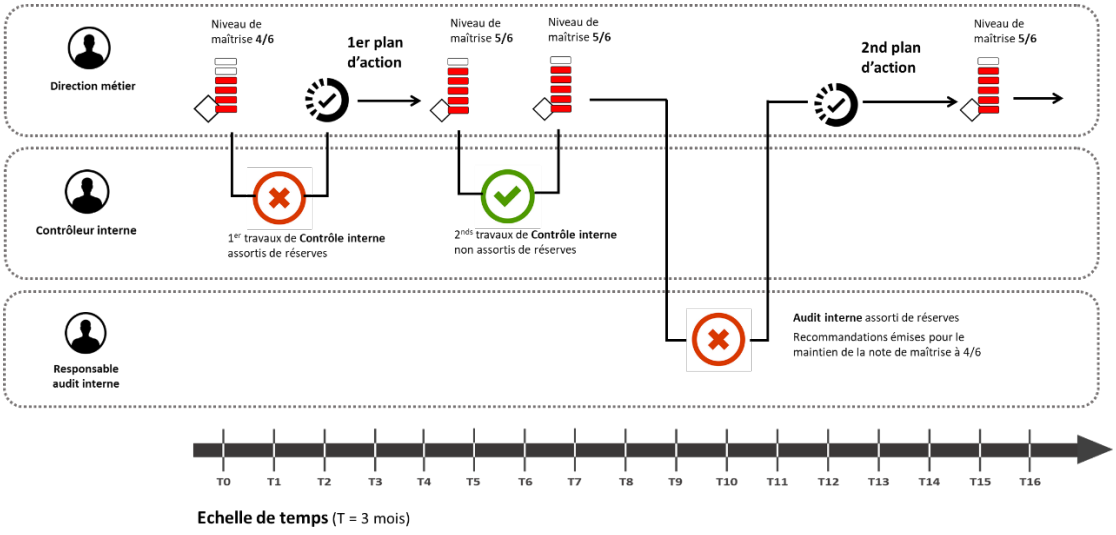
A **T + 12 mois**, ce plan d'action est mené à terme, ce qui justifie la réévaluation du degré de maîtrise à 4+ (« Supervisé+ »).

A **T + 18 mois**, le responsable du contrôle interne s'assure de la robustesse et de l'efficience des dispositifs de maîtrise au moyen de vérifications ponctuelles ; à l'issue de ces travaux il confirme l'évaluation du degré de maîtrise à 4+ (« Supervisé+ »).

A **T + 30 mois**, le responsable de l'audit interne mène à bien une mission d'audit sur la gestion de ce risque particulier qui aboutit à des réserves sur le degré de maîtrise affiché ; il émet des recommandations dont la mise en œuvre conditionne son maintien à terme.

A **T + 36 mois**, le service métier propriétaire du risque conduit un nouveau plan d'action qui répond spécifiquement aux observations émises par le responsable de l'audit interne.

A **T + 45 mois**, ce nouveau plan d'action est clôturé, ce qui permet de lever les réserves émises sur le degré de maîtrise à 4+ (« Supervisé+ »).



Visualiser, mesurer et piloter dans un environnement en évolution constante

En dernier ressort et au terme de ce processus, une collectivité peut être en mesure de recenser et hiérarchiser l'ensemble des risques auxquels elle se trouver exposée et d'établir une **Fiche de suivi et de traitement** de chacun de ces risques où se seront regroupés la totalité des éléments concourant à leur pilotage spécifique.

Ces Fiches de suivi et de traitement doivent être réalisées et renseignées de manière à assurer une parfaite traçabilité des opérations ayant contribué à l'évaluation initiale et à l'éventuel ajustement - par le haut ou par le bas - du degré de criticité ainsi que du niveau de maîtrise des risques constitutifs de la cartographie de la collectivité et, le cas échéant, des organismes associés.

Or la parfaite traçabilité des opérations concourant à la maîtrise globale des risques est un élément essentiel de l'auditabilité de la collectivité, tant vis-à-vis d'auditeurs internes qu'aux yeux de tout auditeur externe habilité.

En conséquence, une collectivité ayant fait le choix de conduire un processus complet de recensement et de pilotage de ses risques nets peut légitimement attendre un gain de confiance à l'endroit de sa gestion, de sa gouvernance et plus généralement de sa capacité à mettre en œuvre les politiques dont elle est chargée.

Ce faisant, elle se donne les moyens de remplir au mieux les attentes des usagers, des agents et de son partenariat élargi en matière de conformité, d'efficacité et de reporting[96] ; elle se trouve ainsi placée sur une trajectoire vertueuse qui doit avoir pour effet d'élargir ses marges d'action et d'offrir à l'exécutif de nouveaux leviers pour un engagement plus ambitieux au bénéfice des territoires et de leurs habitants.

→ Voir **Fiche technique 17**

Exemple de Fiches de suivi et de traitement des risques (criticité/maitrise)

Déploiement d'un outil de pilotage intégré

Afin de pouvoir aisément consolider l'ensemble de ces données et de les exploiter dans une perspective assurantielle de moyen et long terme, une collectivité peut trouver intérêt à se doter d'un outil intégré le management des risques et de pilotage de ses contrôles et audits.

Un tel outil - connu sous l'appellation générique de Système d'information de gestion des risques (SIGR) - a pour objet de faire reposer la programmation et le suivi des campagnes de contrôle et d'audit internes sur une évaluation exhaustive et continuellement actualisée des risques prioritaires et des moyens de maîtrise existants.

Il peut être développé en interne ou acquis.

Dans ce dernier cas, une bonne pratique est pour la collectivité de se conformer autant que possible aux fonctionnalités proposées plutôt que de demander une version entièrement reconfigurée qui générerait des coûts de maintenabilité importants et passerait généralement à côté des améliorations apportées à la version principale.

[96] Voir plus haut, Section 1-A-1

Les éléments ainsi collectés et traités ont vocation à alimenter une démarche d'analyse prospective pour le choix des travaux les plus à même de réduire la vulnérabilité de la collectivité aux principaux risques identifiés, dans les limites fixées par son appétence générale et selon les degrés de tolérance propres à chacune de ses activités.

La Direction générale en déduira également l'existence éventuelle de zones de risques mobilisant des moyens de maîtrise excessifs au regard de l'enjeu pour la collectivité et, le cas échéant, recommander leur réallocation pour tout ou partie au profit d'autres risques à forte criticité potentielle et insuffisamment couverts.

De même, l'utilisation partagée de cet outil aura pour effet de faciliter et fluidifier la nécessaire collaboration entre les acteurs des différentes lignes de maîtrise des risques.

Enfin, l'outil a une fonction décisionnelle sur la trajectoire de la collectivité et la soutenabilité du projet administratif et politique porté par l'Exécutif ; il permet que les arbitrages stratégiques et les choix structurants soient réalisés en pleine connaissance de cause et de manière transparente pour l'ensemble des parties engagées.

Ainsi, l'exécutif et la direction générale disposent de l'ensemble des informations requises pour évaluer précisément et en permanence la vulnérabilité de la collectivité aux principaux risques identifiés, ceci afin de pouvoir vérifier le bien-fondé des efforts consentis et, dans le cas contraire, apporter les corrections nécessaires.

Pour résumer…

Toute collectivité est concernée par la mise en œuvre d'une démarche de gestion et contrôle des risques qui s'inscrit dans une dynamique vertueuse de sécurisation et de pilotage en pleine résonance avec les tendances généralement observées, comme cela est rappelé dans la section 1-A.

Pour ce faire, il lui appartient de créer un dispositif assurantiel conforme aux standards applicables au management des risques et à l'audit interne, tels que présentés dans la section 1-B.

Toutefois le succès et la pérennité d'une telle démarche sont conditionnés à son adaptabilité.

A cet effet, il est recommandé à chaque collectivité candidate d'adopter une approche ambitieuse et graduelle, en procédant en trois phases.

Une première **Phase exploratoire** vise à vérifier que les conditions sont réunies pour mener à bien le projet, à repérer les acteurs clés et à identifier d'éventuels éléments exploitables pour démarrer et avancer rapidement, selon les indications données dans la section 2-A.

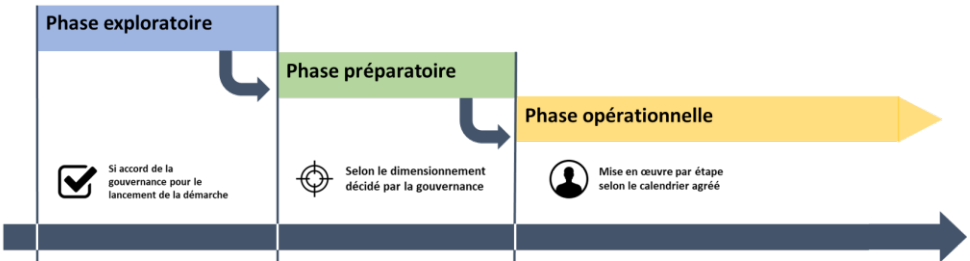
A son issue intervient un arbitrage de la gouvernance quant au bien-fondé de l'entreprise proposée.

Dans le cas où la gouvernance a émis un arbitrage favorable, une seconde **Phase préparatoire** permet d'établir les éléments de méthodologie les mieux appropriés et de définir le périmètre de l'exercice de management des risques, selon les modalités évoquées dans la section 2-B.

En troisième et dernier lieu, une **Phase opérationnelle** correspond à la mise en œuvre des choix précédemment arrêtés ; elle comprend elle-même deux étapes successives.

La première étape - développée dans la section 3-A - est centrée sur la mise en place d'un portefeuille des risques de risques de la collectivité ; elle aboutit à la mise en place d'une cartographie des risques complète et évolutive.

La seconde étape - qui fait l'objet de la section 3-B - tend au déploiement d'une démarche assurantielle couvrant l'ensemble des intérêts de la collectivité, sur le moyen et long terme.



	Phase exploratoire	Phase préparatoire	Phase opérationnelle
Qui ?	**Mission exploratoire** Désignation d'un agent de la collectivité chargé de conduire l'étude préalable	**Mission de préfiguration** Désignation d'un préfigurateur Mise en place d'une équipe-projet	**Création d'une équipe pérenne dédiée** Désignation d'un manageur des risques Désignation des référents métier (propriétaire des risques) Mise en place des fonctions de contrôle et éventuellement d'audit interne
Travaux	▪ Analyse des besoins de la collectivité (notamment au regard des dispositions réglementaire en vigueur) ▪ Evaluation des prérequis pour le déploiement d'une telle démarche (maturité, appétence, culture) ▪ Identification des personnes ressources et le cas échéant des dispositifs partiels existants	▪ Choix de la meilleure entrée pour l'identification des risques ▪ Choix du mode de collecte et d'agrégation le mieux approprié (bottom-up, top-down, mixte…) ▪ Détermination du périmètre de la cartographie (association ou non des organismes satellites) et des familles de risques traitées	**Première étape - Etablir le portefeuille des risques de risques** Quatre jalons successifs : 1. Recenser et documenter les risques de la collectivité 2. Regrouper les risques 3. Evaluer et hiérarchiser les risques 4. Créer les instances de pilotage appropriées (comité des risques…) **Seconde étape - Construire une démarche assurantielle globale** Trois jalons successifs : 1. Mettre en place une fonction d'audit 2. Etablir et mener à bien un programme d'audit adossé à la cartographie des risques 3. Créer les instances de pilotage appropriées (comité d'audit…)
Livrables	Proposition pour arbitrage de création - ou non - d'un dispositif de gestion et contrôle des risques	Proposition de méthodologie pour le déploiement de la cartographie des risques	Cartographie des risques régulièrement actualisée Travaux d'audit permettant de fonder une assurance raisonnable sur la qualité de gestion et la capacité de la collectivité à atteindre les objectifs contenus dans le projet de mandat

CONCLUSION

Dans ces temps incertains et complexes, les collectivités territoriales se trouvent en première ligne pour affronter des urgences de toute nature et assurer les services indispensables à la vie quotidienne.

Auprès de leurs populations respectives, elles sont garantes de la continuité du vivre ensemble mais aussi porteuses de politiques qui tracent des perspectives pour l'avenir et donnent confiance dans le présent.

C'est assez dire qu'il leur revient plus que jamais de faire preuve d'audace et de responsabilité.

De ce fait, elles n'ont pas les moyens d'une politique de l'autruche qui consisterait à ignorer délibérément les principaux risques associés à leur action - ou inaction - dans le champ de leurs compétences respectives en spéculant sur les vertus de l'improvisation ou même sur le secours ô combien aléatoire et fragile de la chance.

A l'inverse, il n'est pas question qu'elles s'abstiennent de toute initiative de peur de s'exposer aux potentielles conséquences fâcheuses qu'entraîne presque nécessairement toute entreprise collective.

Entre ces deux points extrêmes, la sagesse est pour chaque collectivité d'acquérir une connaissance pleine et entière des risques inhérents à l'exercice de ses différentes compétences afin de reconnaître ses principaux points de vulnérabilité et de prendre les mesures correctrices appropriées.

Ce processus d'appropriation et de maîtrise des risques est un enjeu majeur pour des collectivités qui seraient sans cela piégées entre une frilosité paralysante et une témérité inconsciente.

Il s'agit au contraire de considérer l'ensemble des risques susceptibles de survenir à brève ou longue échéance non pas seulement comme des menaces mais aussi comme des opportunités potentielles qui, dûment exploitées, seront autant de leviers nouveaux pour l'action.

Sur cette base, la Direction générale sera en mesure de maintenir une assurance raisonnable quant à la qualité de gestion et - au-delà de cela - sur la capacité de la collectivité à respecter ses obligations et atteindre les objectifs du projet de mandat.

Or le succès d'une telle démarche est conditionné à trois facteurs essentiels.

En premier lieu, elle doit être exactement proportionnée aux besoins et aux objectifs de chaque collectivité.

Il est en effet bien évident que l'ensemble des collectivités ne sont pas soumises aux mêmes obligations réglementaires en termes de pilotage des risques ; en outre et sans qu'il soit besoin de s'étendre sur la disparité de leurs moyens respectifs, chacune se distingue en termes de maturité, de culture et d'appétence aux risques.

Ces éléments déterminants doivent être pris soigneusement en compte pour la mise en place de solutions les mieux adaptées.

En second lieu, elle doit être fermement et durablement portée par les instances dirigeantes de la collectivité, en pleine connaissance de ses effets sur les processus décisionnels futurs et plus largement sur ses modalités de pilotage stratégique et opérationnel.

La mise en place d'une cartographie des risques majeurs associé à un pilotage fin des mesures de maîtrise afférentes est un moyen privilégié pour donner à l'Exécutif et la Direction générale une visibilité accrue sur leurs marges de manœuvre respectives - tant en termes de restrictions que de ressources additionnelles - et apporter à chaque décision un large éclairage pris au sein de la collectivité et dans son environnement étendu.

Il est ainsi nécessaire que les responsables politiques et administratifs de chaque collectivité s'approprient graduellement cet outil et le banalisent au point de l'intégrer à son fonctionnement ordinaire ; ils doivent le faire sans réserve et avec le souci d'impliquer tous les échelons de responsabilité, depuis les services opérationnels jusqu'aux instances stratégiques et décisionnelles.

En troisième et dernier lieu, elle doit avoir l'adhésion de l'ensemble des parties concernées, tout au long de sa phase d'élaboration et de déploiement.

Cette adhésion sera notamment acquise par la mise en partage d'informations parfaitement tracées et transparentes.

De même, il importe que soit adoptée une méthodologie inclusive et participative qui puisse être aisément appréhendée tant au regard de l'objectif à atteindre que des étapes pour y parvenir.

Enfin, la Direction générale doit avoir soin de fixer dès la phase de démarrage les rôles et responsabilités de chaque acteur dans la conduite du projet, de sorte que chacun ait une idée exacte de la contribution attendue de sa part et des éventuelles interactions requises avec d'autres partenaires internes ou externes.

Ainsi l'objet premier de la présente publication est de sensibiliser les collectivités aux enjeux et modalités d'une démarche assurantielle de gestion et maîtrise des risques.

Les éléments ici présentés constituent une guidance pour mener une réflexion d'ensemble sur son bien-fondé et ses implications de tous ordres.

Cette réflexion devra envisager les différents prérequis pour la pleine réalisation d'une entreprise aussi structurante et chargée de sens, notamment au regard des points qui précèdent.

Pour toute collectivité qui souhaitera s'engager plus avant dans ce projet, notre souhait est qu'elle y trouvera également des outils utiles pour avancer et en particulier pour apporter des gages de réussite dès sa phase de démarrage.

A cet effet, nous nous sommes inspirés des meilleures pratiques observées dans les collectivités ayant déjà développé des fonctions de management des risques, de contrôle interne et d'audit interne.

Nous avons également pris appui sur de précédents travaux à visée professionnelle et avons capitalisé sur leurs acquis méthodologiques et techniques, dans une logique d'amélioration continue.

Notre propos est ainsi de fournir une aide à chaque collectivité prise individuellement en lui apportant ce qui lui est nécessaire pour se déterminer sur les dispositions à prendre en matière de management et de maîtrise de ses risques, dans la situation particulière où elle se trouve et sans préjuger de ses besoins spécifiques.

Nous nous adressons aux collectivités encore situées très en amont d'une telle démarche comme aux collectivités ayant déjà partiellement développé des fonctions de management des risques ; de même nous ne nous bornons pas aux collectivités dotées d'une fonction d'audit et avons l'ambition d'être pareillement utiles à celles qui en sont dépourvues.

A chacune d'entre elles nous souhaitons fournir quelques bases pratiques et théoriques communes qui pourront être réutilisées et exploitées pour alimenter des travaux prospectifs ; dans le cas des collectivités plus avancées, des éléments sont disponibles pour faciliter et accompagner le lancement de missions de préfiguration voire pour préparer la création de fonctions pérennes dédiées au management des risques, au contrôle interne ou à l'audit interne.

Pour toutes les collectivités ayant passé la phase d'arbitrage et tranché dans le sens d'un engagement dans la démarche, ces bases communes sont également susceptibles de contribuer aux spécifications métier requises pour le développement ou l'acquisition d'outils de pilotage dédiés à la gestion et à maîtrise des risques.

Ce faisant, notre seul dessein est de promouvoir une culture de la gestion du risque au sein des collectivités au travers de méthodes et outils tournés vers l'expérimentation.

Nous gageons que les résultats obtenus parleront d'eux-mêmes pour susciter de nouvelles initiatives par la force de l'exemple et la pédagogie du faire pour apprendre.

Nous espérons enfin avoir montré l'intérêt qu'il y a pour tout type de collectivité de mettre en œuvre une démarche assurantielle robuste et pérenne intégrant plusieurs lignes de maîtrise, quitte à mutualiser tout ou partie des ressources requises pour les plus petites d'entre elles.

Si ce but est atteint, nos efforts auront été amplement justifiés et récompensés.

Glossaire

Le vocabulaire de la connaissance et de la maîtrise des risques

Appétence au risque

Il s'agit de la part de risque qu'une organisation est prête à assumer dans ses missions et dans ses prises de décisions pour asseoir et finaliser sa stratégie au regard d'objectifs définis.

La définition de l'appétence au risque permet de définir le niveau de maitrise à atteindre par l'organisation et éviter de mettre en œuvre des contrôles excessifs au regard de risques mineurs et/ou assumés.

L'appétence au risque correspond ainsi à une balance entre le coût de la maîtrise d'un risque et les éventuels avantages directs ou indirects attachés au fait de tolérer ce même risque.

Cette appréciation dépend des inclinaisons de la gouvernance et peut évoluer dans le temps, en particulier à chaque changement ou renouvellement de mandat.

Assurance raisonnable

L'assurance raisonnable est une garantie susceptible d'être donnée à la gouvernance quant à la bonne gestion de l'organisation et la soutenabilité des objectifs contenus dans le projet de mandat et le projet d'administration subséquent.

Cette garantie repose sur la mise en place de mesures de maîtrise des principaux risques suffisantes et reconnues comme efficaces.

Il appartient à la troisième ligne de maîtrise des risques (audit interne) de vérifier la robustesse des mesures de maîtrise existantes et, dans le cas où des dysfonctionnements seraient constatés, de proposer les actions correctrices les mieux appropriées.

L'assurance raisonnable est donc apportée par le Responsable de l'audit interne au regard des résultats de ses travaux et des suites données par les directions métier concernées ; si ces éléments ne sont pas concluants, le Responsable de l'audit interne est fondé à ne pas la donner jusqu'à la mise en œuvre effective des corrections attendues.

Audit assurantiel

Les audits assurantiels concernent les risques à forte criticité et à fort degré de maîtrise.

Ils ont pour objet de vérifier la robustesse des mesures de maîtrise mises en place en réponse à ces risques et ainsi d'attester - ou corriger - le degré d'assurance susceptible d'être donné sur la capacité de l'organisation à contenir et le cas échéant surmonter les menaces inhérentes.

Audit conseil

Les audits conseils sont quant à eux réalisés sur les risques à forte criticité et à faible degré de maîtrise.

Leur propos est de rechercher des voies pour réduire l'exposition de l'organisation à ces risques, au regard de l'enjeu qu'ils représentent pour la collectivité et des moyens de maîtrise susceptibles d'être mobilisés et/ou redéployés.

Audit de conformité

Les audits de conformité visent à vérifier la correcte application de règles et procédures auxquelles est astreinte une organisation.

En cas de non-application ou d'application imparfaite, des recommandations sont émises pour le rétablissement à brève échéance d'une situation satisfaisante.

Dès lors que l'organisation est présumée se conformer aux règles et procédures concernées, les audits de conformité prennent la forme d'audits assurantiels ; dans le cas contraire, ils s'apparentent à des audits conseils.

Audit interne

L'audit interne est une activité indépendante et objective qui doit donner à une organisation une assurance sur le degré de maîtrise de ses opérations et lui apporter tout conseil utile pour les améliorer ; ce faisant il contribue à créer de la valeur ajoutée au bénéfice de l'ensemble des parties engagées.

Plus généralement, l'audit interne a pour vocation d'aider l'organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques et de contrôle.

Auto-évaluation du contrôle interne

Il s'agit d'une procédure de sécurisation des travaux de contrôle interne au travers de l'obligation faite à chaque contrôleur d'évaluer par lui-même la fiabilité des vérifications dont il a la charge.

Cet exercice est conduit à tout niveau, en fonction des objectifs et des risques identifiés par l'organisation et par l'opérationnel lui-même.

La démarche d'auto-évaluation est initiée par la Direction Générale et mise en œuvre par les opérationnels.

Cartographie des risques

Cette formulation désigne un outil d'analyse et de communication graphique qui aide à recueillir les vulnérabilités et à évaluer la pertinence des actions à mettre en place pour les traiter.

Selon le modèle le plus usité, la vulnérabilité se décompose en deux valeurs permettant de mesurer la probabilité et l'impact potentiel du risque.

Chaque risque est positionné au regard de ces deux valeurs qui sont représentées sur les deux axes d'un diagramme.

Catégories d'objectifs

Il s'agit des objectifs que poursuit une organisation et dont la réalisation est susceptible d'être menacée du fait de risques particuliers.

Ces objectifs sont regroupés en quatre grandes familles, selon la nomenclature proposée par le référentiel COSO (voir plus bas), soit :

- des objectifs stratégiques ;
- des objectifs opérationnels liés la réalisation et l'optimisation des travaux incombant à l'organisation ;
- des objectifs relatifs à la fiabilité des reportings (financiers et autres) ;
- des objectifs ayant trait à la bonne application des lois et réglementations en vigueur.

Cause principale

Ce terme décrit les principaux facteurs à l'origine de la survenance d'un risque.

Une cause principale est aussi dite « cause racine »

Contrôles de premier niveau

Il s'agit des contrôles opérationnels et la surveillance permanente effectués par chaque collaborateur et sa hiérarchie dans le cadre naturel de leurs activités quotidiennes.

Ces contrôles permettent d'assurer que les tâches inhérentes à un processus opérationnel ou support ont été effectuées conformément aux procédures édictées par l'entité contrôlée.

Contrôles de second niveau

Il s'agit de contrôles réalisés *a posteriori*, à fréquence prédéfinie ou aléatoire, dans la mesure du possible par des services non impliqués de manière opérationnelle.

Ces contrôles sont des contrôles de fond et de forme permettant de vérifier la correcte exécution des contrôles de premier niveau et le bon fonctionnement du dispositif existant.

Contrôles de troisième niveau

Il s'agit de contrôles et investigations menés à l'initiative du Responsable de l'audit interne et sous sa supervision afin d'établir une assurance raisonnable quant à la qualité de gestion de la collectivité et la correcte maîtrise des risques pesant sur son fonctionnement et son action.

Contrôle de gestion

Il s'agit d'un processus de pilotage conçu pour aider le responsable d'un service gestionnaire à atteindre ses objectifs.

Cette démarche vise à préparer, suivre et analyser - à la fois en temps réel et ex-post - les réalisations de son service et de ceux qui lui sont rattachés, pour anticiper, expliquer et réduire les écarts entre ses performances et ses prévisions.

Contrôle interne

Il s'agit d'un dispositif de l'organisation visant à lui donner les moyens d'une meilleure maîtrise de ses activités, à renforcer l'efficacité de ses opérations et à assurer une utilisation plus efficiente de ses ressources.

Le contrôle interne contribue ainsi à limiter les risques de non-atteinte des objectifs que s'est fixés l'organisation et apporte des informations clé pour la conduite et le pilotage de ses différentes activités.

Le contrôle interne porte notamment sur :

- la conformité aux lois et règlement ;
- l'application des instructions et des orientations fixées par la gouvernance ;
- le bon fonctionnement des processus internes de l'organisation ;
- la fiabilité des informations financières.

Toutefois, le contrôle interne ne peut fournir une garantie certaine que les objectifs de l'organisation seront atteints.

COSO

COSO est l'acronyme de Committee of Sponsoring Organizations of the Treadway Commission

Il s'agit d'un référentiel de contrôle interne mis en place en 1992 dans le but de limiter les tentatives de fraudes dans les rapports financiers des entreprises.

En juillet 2002, le Congrès des Etats-Unis a adopté une loi dite Sarbanes - Oxley (ou SOX Act) qui fait obligation à toutes les sociétés faisant appel à l'épargne publique à évaluer leur contrôle interne et à en publier leurs conclusions en prenant appui sur le référentiel COSO.

En France, la loi de sécurité financière promulguée en août 2003 a repris ces dispositions, ce qui a favorisé sa diffusion comme outil de travail commun aux différentes autorités de contrôle et de certification.

Le référentiel initial (COSO 1) a évolué vers un second corpus (COSO 2) plus fortement axé sur le management des risques et le pilotage de la performance.

Criticité

La criticité d'un risque est une combinaison de sa probabilité et de son impact potentiel.

Démarche assurantielle

Il s'agit d'un dispositif de gestion et de contrôle des risques établi à l'échelle d'une organisation qui permet de donner à la gouvernance une assurance raisonnable quant à sa bonne gestion et à l'atteinte des objectifs qu'elle s'est fixés.

La mise en place d'une démarche assurantielle implique le déploiement d'une démarche globale de mangement des risques et la création d'une fonction d'audit interne assurant les contrôles de troisième niveau.

Direction métier

Voir ci-après « Propriétaire de risque »

Facteurs de risque

Cette expression désigne les causes possibles d'un évènement susceptible d'avoir des conséquences néfastes pour l'organisation.

La détermination de ces causes permet en particulier de mesurer sa probabilité et d'agir préventivement au moyen de mesures de maîtrise appropriées.

Fiche de risque

Il s'agit d'un document-type permettant de présenter individuellement chacun des risques auxquels est exposée une organisation donnée.

Un tel support doit permettre *a minima* de restituer :

- son positionnement dans un processus métier ;
- la direction métier propriétaire ;
- son degré de criticité.

Le cas échéant, il est opportun d'ajouter :

- des éléments de reporting des plans d'action menés en vue de renforcer son degré de maîtrise ;
- les recommandations des contrôles et/ou audits qui s'y rapportent.

L'ensemble de ces informations doivent être rendues disponibles avec un degré de traçabilité aussi élevé que possible.

Impact

Ce terme désigne l'effet positif ou négatif d'un évènement sur la réalisation des objectifs de l'organisation.

Un même évènement peut se traduire par différents impacts possibles.

A titre d'exemple, l'application d'une correction forfaitaire du fait d'une gestion déficiente de crédits de la politique européenne de cohésion peut avoir pour la même collectivités un impact en termes financiers ou en termes d'image...

Chacun de ces impacts est ainsi susceptible d'être évalué en appui d'indicateurs spécifiques permettant de mesurer le coût financier d'un événement, son incidence sur la qualité du service rendu (mesuré en termes de satisfaction des usagers…).

Limites inhérentes

Il s'agit des facteurs humains et matériels non maîtrisables qui écartent toute possibilité d'infaillibilité du contrôle interne et maintiennent l'organisation dans une situation d'incertitude relative quant à l'atteinte des objectifs qu'elle s'est fixés.

Cette part incompressible d'aléa fait que toute assurance donnée sur ce point ne peut être que raisonnable et en aucune manière absolue.

Maîtrise d'un risque

Il s'agit des différentes mesures prises pour limiter la probabilité et/ou les impacts potentiels d'un risque.

On distingue en particuliers deux types de mesures de maîtrise :

- les mesures de maîtrise préventives qui visent particulièrement à diminuer la fréquence du risque ;
- les mesures de maîtrise correctives qui ont surtout pour objet de réduire son impact.

Un même risque peut faire concurremment l'objet de mesures de maîtrise préventives et correctives, selon l'appréciation de la gouvernance.

Niveau de revue

Il s'agit d'une échelle à trois paliers précisant l'identité du vérificateur de la criticité d'un risque sur le modèle des trois lignes de maîtrise.

Les trois paliers existants sont ainsi par ordre d'assurance croissant :

- déclaré métier, criticité du risque appréciée par la direction métier propriétaire ;
- revue contrôle interne, criticité du risque testée et vérifiée par contrôle interne ;
- revue audit (interne et/ou externe) criticité du risque testée et validée par le Responsable de l'audit interne et/ou tout auditeur externe habilité.

Organisation

Ce terme désigne toute forme sociale créée pour un besoin spécifique.

Outre une collectivité, on peut citer à titre d'exemple une organisation commerciale, une société à but non lucratif, un établissement d'enseignement…

Les autres termes employés en tant que synonymes sont « société » et « entité ».

Portefeuille de risques

Il s'agit de l'ensemble des risques attribués à une même direction métier, désignée en tant que leur propriétaire.

Processus

Il s'agit d'un ensemble organisé de moyens et d'activités qui transforment des éléments entrants en éléments sortants en y apportant une valeur ajoutée.

On distingue généralement trois types de processus :

- les processus « Métiers » (ou de réalisation) représentant l'offre de services de l'organisation ;
- les processus « Stratégiques » (ou de direction) qui définissent les règles, les stratégies et les plans qui gouvernent les processus Métiers ;
- les processus « Supports » qui permettent la mise œuvre des processus « Métiers ».

Chacun des risques pensant sur une organisation donnée est rattachable à un processus (ou process) particulier ; le fait de l'inscrire dans une chaine de traitement précisément décrite permet de mieux identifier ses causes et ses conséquences éventuelles.

Processus de management des risques

Il s'agit de l'ensemble des actions entreprises par le management pour identifier des évènements potentiels susceptibles d'affecter la vie de l'organisation, gérer les risques qui y sont attachés et fournir une assurance raisonnable que ses objectifs seront atteints.

Le management des risques de l'organisation fait partie intégrante du processus de management global.

Processus de contrôle

Cette expression désigne les politiques, procédures et activités faisant partie d'un système de contrôle, conçus pour assurer que les risques sont contenus dans les limites fixées par la gouvernance.

Propriétaire du risque

Agent directement responsable du processus auquel est rattaché un risque et chargé à ce titre d'une stratégie de réponse pour maintenir ce risque à un niveau de criticité reconnu acceptable par la gouvernance.

Selon le ou les processus dont il est garant, chaque propriétaire de risques est ainsi amené à gérer et piloter un portefeuille constitué de l'ensemble des risques y afférents.

Le propriétaire du risque peut également prendre le nom de « Direction métier ».

Risque

Ce terme désigne la possibilité que se produise un évènement susceptible d'avoir un impact sur la réalisation des objectifs de l'organisation.

Un risque est caractérisé par deux types d'éléments :

- un ensemble de causes et de conséquences particulières qui s'inscrivent dans un processus métier déterminé ;
- un niveau de maîtrise résultant de l'effet combiné de mesures préventives et/ou correctrices dédiées.

Sur la base de ces éléments, chaque risque se mesure en termes de probabilité et d'impact potentiel.

Risque cible

Il s'agit de la somme des conséquences qu'une organisation est prête à accepter, liée à la probabilité de la survenance d'un évènement indésirable.

Ce maximum tolérable se mesure en termes de criticité du ou des risque(s) concerné(s).

Il varie en fonction de l'appétence aux risques de l'organisation.

Celle-ci peut ainsi ambitionner de diminuer l'impact et la probabilité d'un risque et d'en renforcer la maîtrise, afin d'atteindre des conditions qu'elle juge acceptables ; dans ce cas la criticité-cible du risque diminue et le propriétaire du risque est amené à mettre en œuvre des mesures de maîtrise additionnelles dans le cadre d'un plan d'action dédié.

Risque endogène

Il s'agit d'un évènement survenant au sein de l'organisation impactant la réalisation d'objectifs déterminés.

Les risques endogènes appellent des stratégies de réponse mobilisant prioritairement les ressources de l'organisation ; ces stratégies prennent la forme de mesures de maîtrise préventive et/ou corrective pilotées en interne et intégrées au fonctionnement des services.

Risque exogène

Il s'agit d'un évènement survenant au sein de l'organisation impactant la réalisation d'objectifs déterminés.

Les risques endogènes appellent des stratégies de réponse appropriées qui insistent particulièrement sur les mesures de corrective puisque leurs facteurs de survenance échappent à l'organisation.

Risque brut

Il s'agit d'un risque considéré en termes de probabilité et d'impact potentiel sans tenir compte de l'effet des dispositifs de maitrise et de contrôle qui l'entourent.

A titre d'exemple, un risque financier observé tel quel et donc sans le dispositif de maîtrise mis en place par le contrôle interne est un risque brut.

Un risque brut peut aussi être dit « risque inhérent » ou « risque initial ».

Risque net

Il s'agit d'un risque considéré en termes de probabilité et d'impact potentiel après prise en compte des dispositifs de maîtrise et des mesures d'atténuation dédiées.

Un risque net peut aussi être dit « risque résiduel ».

Vraisemblance

Il s'agit de la probabilité de survenance d'un événement reconnu comme un risque pour l'organisation.

Elle doit être établie au regard d'une période de référence et d'éléments de quantification de l'événement décrit afin d'établir un cadre temporel ou quantitatif précis.

Il est à noter que la vraisemblance d'un événement sur une période de temps indéterminée tend systématiquement vers une quasi-certitude ; à l'inverse, si elle est mesurée dans un cadre temporel défini, sa possibilité de survenance est plus contenue, elle peut donc être mesurée et rapportée à la gouvernance en vue de projections réalistes à un horizon de temps dans son périmètre de maîtrise.

Vulnérabilité

Ce terme décrit le degré de fragilité d'un système particulier, qu'il s'agisse d'une entité organisationnelle, d'un processus métier ou d'un projet.

La vulnérabilité peut être établie par le produit de la vraisemblance et de l'impact divisé par le degré de maîtrise.

Plus un système est vulnérable, plus la gouvernance doit lui porter attention et le cas échéant demander qu'il fasse l'objet de mesures de maîtrise additionnelles.

Fiches techniques

Liste des Fiches techniques

1) Cadre réglementaire des collectivités territoriales en matière de déontologie et de prévention des conflits d'intérêts (+ 2 annexes)

2) Recommandations de l'AFA relatives à la prévention et à la détection des actes contraires à la probité (+ 2 annexes)

3) Obligations liées à la mise en œuvre des financements de la politique européenne de cohésion

4) Expérimentation de la certification des comptes dans les collectivités locales (2017-2023)

5) Mode opératoire pour la mise en place d'un système de management de la continuité d'activité

6) Le processus de management du risque

7) Les trois lignes de maîtrise des risques

8) Profils engagés dans une démarche de maîtrise des risques - Acteurs en charge de la gouvernance

9) Profils engagés dans une démarche de maîtrise des risques - Acteurs en charge des trois lignes de maîtrise

10) Risques le plus fréquemment rencontrés et exemples d'univers de risques dans différents types de collectivités

11) Outils & méthodes d'évaluation des risques présentés dans la Norme ISO 31000 relative au management des risques (+ 3 annexes)

12) Exemples d'échelles de criticité des risques

13) Proposition pour la mise en place d'une échelle de maîtrise des risques

14) Normes professionnelles de l'audit interne

15) Rôle de l'audit interne dans le management des risques

16) Le tableau MARCI comme outil de pilotage des audits

17) Exemple de Fiche synthétique de suivi et de traitement d'un risque (criticité/maitrise)

Fiche technique 1

Cadre réglementaire des collectivités territoriales en matière de déontologie et de prévention des conflits d'intérêts

I. Principes généraux

Les obligations de déontologie qui s'imposent aux élus comme aux agents des collectivités territoriales découlent des missions de service public dont ils sont particulièrement chargés.

Ces obligations s'ajoutent au régime de responsabilité attaché à l'exercice d'activités professionnelles et aux droits et obligations réciproques entre employeur et salariés.

Elles touchent prioritairement à un éventuel usage abusif des pouvoirs qui sont accordés à certains élus et agents pour l'exercice de leurs missions en vue de les détourner à des fins personnelles ou pour le compte d'intérêts extérieurs à la collectivité.

Les atteintes à la déontologie ont d'abord vocation à être réprimées par la procédure disciplinaire mise en œuvre par l'autorité territoriale.

En outre et dans un cadre pénal, différents délits ont été créés pour caractériser et punir ces abus - voir Annexe 1

Plus largement, la notion de déontologie renvoie à l'adoption d'attitudes éthiques et à une demande d'exemplarité de la part d'élus et d'agents œuvrant pour le bien commun et mandatés à cette fin.

Les premières exigences posées en la matière concernent les agents publics.

Dispositions relatives à la déontologie agents publics

Dans ses articles L. 121-1 à 11 et L. 124-1[97], le Code général de la fonction publique fixe le comportement attendu des agents publics dans l'exercice de leurs fonctions.

Dans leur version actuelle, ces articles sont ainsi libellés.

« *Le fonctionnaire exerce ses fonctions avec dignité, impartialité, intégrité et probité.*

Dans l'exercice de ses fonctions, il est tenu à l'obligation de neutralité.

Le fonctionnaire exerce ses fonctions dans le respect du principe de laïcité. A ce titre, il s'abstient notamment de manifester, dans l'exercice de ses fonctions, ses opinions religieuses.

Le fonctionnaire traite de façon égale toutes les personnes et respecte leur liberté de conscience et leur dignité. (…)

Il appartient à tout chef de service de veiller au respect de ces principes dans les services placés sous son autorité. Tout chef de service peut préciser, après avis des représentants du personnel, les principes déontologiques applicables aux agents placés sous son autorité, en les adaptant aux missions du service. »

[97] Ces articles sont issus de l'article 25 de la loi n° 83-634 du 13 juillet 1983 dite « loi Le Pors » complétée par la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires et la loi n° 2019-828 du 6 août 2019 de transformation de la fonction publique

Ultérieurement, un corpus déontologique à destination des élus s'est mis en place.

Ce corpus est le fondement de chartes de déontologie désormais largement répandues.

Dispositions relatives à la déontologie des élus

La loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique dispose dans son article premier :

« *Les membres du Gouvernement, les personnes titulaires d'un mandat électif local ainsi que celles chargées d'une mission de service public exerce leurs fonctions avec dignité, probité et intégrité et veillent à prévenir ou à faire cesser immédiatement tout conflit d'intérêts*. »

Dans son article second, la loi n° 2015-366 du 31 mars 2015 visant à faciliter l'exercice, par les élus locaux, de leur mandat explicite ces prescriptions et créée une Charte de l'élu local[98] ainsi libellée.

« *L'élu local exerce ses fonctions avec impartialité, diligence, dignité, probité et intégrité.*

Dans l'exercice de son mandat, l'élu local poursuit le seul intérêt général, à l'exclusion de tout intérêt qui lui soit personnel, directement ou indirectement, ou de tout autre intérêt particulier.

L'élu local veille à prévenir ou à faire cesser immédiatement tout conflit d'intérêts. Lorsque ses intérêts personnels sont en cause dans les affaires soumises à l'organe délibérant dont il est membre, l'élu local s'engage à les faire connaître avant le débat et le vote.

L'élu local s'engage à ne pas utiliser les ressources et les moyens mis à sa disposition pour l'exercice de son mandat ou de ses fonctions à d'autres fins.

Dans l'exercice de ses fonctions, l'élu local s'abstient de prendre des mesures lui accordant un avantage personnel ou professionnel futur après la cessation de son mandat et de ses fonctions.

L'élu local participe avec assiduité aux réunions de l'organe délibérant et des instances au sein desquelles il a été désigné.

Issu du suffrage universel, l'élu local est et reste responsable de ses actes pour la durée de son mandat devant l'ensemble des citoyens de la collectivité territoriale, à qui il rend compte des actes et décisions pris dans le cadre de ses fonctions. »

II. Une suite de textes législatifs et réglementaires ont eu pour effet de renforcer les règles de déontologie applicables aux collectivités

Un ensemble de règles normatives s'est graduellement mis en place pour encadrer l'action des collectivités dans le sens d'une attention croissante aux questions de probité et faciliter l'adoption de pratiques déontologiques en accord avec les attentes du public.

Les règles ainsi créées répondent pour l'essentiel aux finalités suivantes :

- faciliter l'accès des administrés aux actes, documents et décisions susceptibles de leur être opposés afin de favoriser l'exercice de leurs droits ;
- prévenir les situations de conflits d'intérêts ;
- organiser et protéger le signalement d'actes potentiellement délictueux.

[98] Cette Charte est insérée dans l'article 1111-1-1 du Code général des collectivités territoriales

A. Dispositions relatives à la transparence des actes et décisions

L'obligation faite à toute administration de motiver en faits et en droit les décisions prises à l'encontre des usagers ou des agents de la fonction publique est le produit de décisions anciennes et constantes du juge administratif.

Elle a été plus récemment reprise et codifiée par le législateur, comme en témoigne la loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public.

De nouvelles dispositions se sont ajoutées pour renforcer et donner les garanties données quant à un traitement impartial et équitable de tout cas individuel.

L'article 24 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations prévoit ainsi que les décisions individuelles n'interviennent qu'après que la personne intéressée soit à même de présenter des observations écrites et, le cas échéant, sur sa demande, des observations orales.

De nombreux textes ont été publiés dans ce sens jusqu'à l'ordonnance n° 2021-1310 du 7 octobre 2021 portant réforme des règles de publicité, d'entrée en vigueur et de conservation des actes pris par les collectivités territoriales et leurs groupements.

Leur accumulation a d'ailleurs justifié la création d'un Code des relations entre le public et l'administration, suite à l'ordonnance n° 2015-1341 du 23 octobre 2015.

> Voir un tableau récapitulatif des obligations applicables en **Annexe 1**

B. Dispositions relatives à la prévention des conflits d'intérêts

Dans le même temps, des dispositions ont été prises pour limiter les risques de conflits d'intérêts au sein des collectivités.

Ces dispositions revêtent un caractère préventif et visent à écarter toute possibilité d'infraction, soit par méconnaissance, soit par intention délibérée.

> Voir un tableau récapitulatif des obligations applicables en **Annexe 2**

a. Obligation de déport ou d'abstention en cas de conflit d'intérêts

L'article 2 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique définit une situation de conflit d'intérêt comme étant « *toute situation d'interférence entre un intérêt public et des intérêts publics ou privés qui est de nature à influencer ou à paraître influencer l'exercice indépendant, impartial et objectif d'une fonction*. ».

Cette même loi décrit la procédure à suivre en cas de situation de conflit d'intérêt.

Ainsi et dans le cas où une situation de conflit d'intérêts est soupçonnée :

- les membres des collèges d'une autorité administrative indépendante ou d'une autorité publique indépendante doivent s'abstenir de siéger ou de délibérer ;
- les personnes titulaires de fonctions exécutives locales (sous réserve des exceptions prévues au deuxième alinéa de l'article 432-12 du code pénal) doivent être suppléées par leur délégataire sans leur adresser d'instructions ;
- les personnes chargées d'une mission de service public qui ont reçu délégation de signature doivent s'abstenir d'en user ;
- les personnes chargées d'une mission de service public placées sous l'autorité d'un supérieur hiérarchique le saisissent ; ce dernier, à la suite de la saisine ou de sa propre initiative, confie, le cas échéant, la préparation ou l'élaboration de la décision à une autre personne placée sous son autorité hiérarchique.

b. Déclarations de situation patrimoniale et d'intérêts

Conformément aux dispositions de l'article 11 de la loi n°2013-907 du 11 octobre 2013 relative à la transparence de la vie publique et dans les délais prescrits, chaque collectivité doit adresser à la Haute autorité pour la transparence de la vie publique (HATVP) les déclarations de situation patrimoniale et d'intérêts du chef de l'Exécutif (maire, président) comme des élus ayant reçu expressément une délégation de signature.

La HATVP dispose d'un pouvoir de contrôle, de vérification de la sincérité des déclarations d'intérêts et de situation patrimoniale fixé par les articles 19 à 23 de la loi du 11 octobre 2013.

Les articles L 122-2 à 22 du Code général de la fonction publique[99] étendent l'obligation de déclaration de situation patrimoniale et/ou d'intérêts aux fonctionnaires dont la nature des fonctions et le niveau hiérarchique l'exigent.

La liste de ces agents est fixée par le décret n° 2016-1967 du 28 décembre 2016.

Certaines mesures récentes ont pour but de faciliter le signalement d'actes de fraude et de sensibiliser les agents aux principes de déontologie qui leur sont applicables.

Elles prolongent les dispositions de l'article 40 du Code de procédure pénal qui fait obligation à « *toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit […] d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs.* »

[99] Anciennement articles 25 ter à 25 sexies de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires tels qu'issus de l'article 5 de la loi n°2016-483 du 20 avril 2016

c. Création de référents déontologues

La loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires et modifiée par la loi n° 2019-828 du 6 août 2019 de transformation de la fonction publique ouvre le droit à tout agent public de « *consulter un référent déontologue, chargé de lui apporter tout conseil utile au respect des obligations et des principes déontologiques* » ; ce principe a ensuite été codifié à l'article L124-2 du Code général de la fonction publique.

Ces textes imposent aux administrations de créer cette fonction de déontologue selon les modalités édictées par le Décret n° 2017-519 du 10 avril 2017 relatif au référent déontologue dans la fonction publique.

L'article 4 de ce même décret dispose donc des modalités de nomination suivantes :

- Le référent déontologue doit être désigné à un niveau lui permettant l'exercice effectif de ses missions.
- Pour les collectivités publiques relevant de la loi du 26 janvier 1984, le référent déontologue est désigné par l'autorité territoriale. Pour les collectivités territoriales et les établissements publics affiliés à titre obligatoire ou volontaire à un centre de gestion, il est désigné par le président du centre de gestion. Enfin, dans les établissements mentionnés à l'article 4 de la loi du 9 janvier 1986, le référent déontologue est désigné par l'autorité disposant du pouvoir de nomination.
- Une fois nommé, l'article 5 du décret précise que le nom du référent déontologue doit être porté à la connaissance de tout agent par les chefs de service.
- Enfin l'article 6 du décret impose au chef de service de mettre à disposition du référent déontologue tout le matériel nécessaire lui permettant l'exercice de ses fonctions.

En ce qui concerne les devoirs et les missions du référent déontologue :

- l'article 6 du décret lui fait obligation de respecter le secret des échanges et d'une totale discrétion professionnelle ;
- l'article 8 précise qu'en cas de signalement de conflit d'intérêt, le référent déontologue « *apporte aux personnes intéressées tous conseils de nature à faire cesser ce conflit* ».

L'article L 124-2 du Code général de la fonction publique[100] ouvre à tout fonctionnaire le droit « *de consulter un référent déontologue, chargé de lui apporter tout conseil utile au respect des obligations et des principes déontologiques (…) ».* Le même article précise que cette fonction de conseil « *s'exerce sans préjudice de la responsabilité et des prérogatives du chef de service*[101] ».

Le décret n° 2017-519 en date du 10 avril 2017 relatif au référent déontologue dans la fonction publique fixe le mode opératoire de ces dispositions, son entrée en vigueur est fixée au 13 avril 2017.

Ce texte précise que les référents déontologues sont missionnés pour une durée fixée éventuellement reconductible (article 2) et apporte certaines garanties d'un fonctionnement autonome, en particulier en restreignant leur recrutement à des personnalités qualifiées extérieures à la fonction publique, des magistrats et fonctionnaires, en activité ou retraités, ou des agents contractuels bénéficiant d'un contrat à durée indéterminée (article 3) et en prescrivant un positionnement hiérarchique approprié (article 4).

[100] Anciennement article 11 de la loi du 20 avril 2016 qui avait créé un nouvel article 28 [bis] de la loi n° 83-634 du 13 juillet 1983

[101] Ces prérogatives sont notamment rappelées dans les articles L.121 et suivants du Code général de la fonction publique

d. Mise en place de référents laïcité

Une circulaire du Ministre de la fonction publique du 15 mars 2017 relative au respect du principe de laïcité dans la fonction publique[102] a fourni de premières pistes de réflexion utiles pour la mise en pratique de cette nouvelle obligation inscrite dans l'article L. 121-2 du Code général de la fonction publique [103].

Il en ressort en particulier que les conseils en la matière peuvent être indifféremment apportés par un correspondant ou un référent « laïcité » dédié ou par le référent déontologue désigné sur le fondement de l'article L.124-2 du Code général de la fonction publique[104], selon les spécificités des missions et l'organisation de chaque administration.

Ces dispositions ont été reprises et renforcées dans la loi n° 2021-1109 du 24 août 2021 puis codifiées dans l'article L. 124-3 du Code général de la fonction publique confortant le respect des principes de la République qui fait obligation aux collectivités territoriales de désigner en leursein un référent laïcité, au même titre que les administrations de l'Etat et les établissements publics.[105]

Comme il en allait précédemment, les fonctions de référent déontologue et de référent laïcité peuvent être réunies en la même personne.

C. Signalement des actes potentiellement délictueux

L'exercice d'une parcelle de l'autorité publique a pour contrepartie une obligation de vigilance particulière à l'endroit de tout acte potentiellement délictueux qui se traduit par l'obligation d'en assurer le signalement sans délai.

Ce principe établi de longue date a connu de nouveaux développements avec la mise en place du recueil des signalements d'alerte issu de la loi Sapin 2 du 9 décembre 2016.

a. Obligation faite aux élus et aux agents d'informer le ministère public de toute infraction grave dont ils acquièrent la connaissance dans l'exercice de leurs fonctions

Du fait de leur rôle particulier dans la gestion des affaires publiques et des pouvoirs dont ils peuvent disposer au nom de l'intérêt général, un principe pénal ancien charge les agents de l'administration d'alerter personnellement et directement l'autorité judiciaire sur les violations graves du droit (crime ou délit) dont ils sont témoins.

---

[102] Réf. NOR : RDFF1708728C

[103] Anciennement article 25 de la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires.

On y lit : « Le fonctionnaire exerce ses fonctions dans le respect du principe de laïcité. A ce titre, il s'abstient notamment de manifester, dans l'exercice de ses fonctions, ses opinions religieuses »

[104] Issu de la loi n° 2016-483 du 20 avril 2016

[105] Ces dispositions sont intégrées à l'article L 124-3 du Code général de la fonction publique issu de l'article 28 ter de la loi n° 83-634 du 13 juillet 1983

Les critères et modalités de sélection ainsi que les missions des référents référent laïcité dans la fonction publique sont spécifiés dans le décret n° 2021-1802 du 23 décembre 2021.

Ce principe est énoncé dans le second alinéa de l'article 40 du Code de procédure pénale

« *Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs*. »

Les agents publics sont concernés au premier chef, sans qu'il y ait lieu de distinguer selon leur statut de titulaire ou contractuel.

Toutefois, la rédaction présente - issue de l'article 74 de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité - induit que les élus des collectivités territoriales, en tant que représentants d'autorités constituées, sont astreints à la même obligation.

Il convient d'y ajouter les dispositions du premier alinéa de l'article L 2211-2 du Code général des collectivités territoriales[106] qui prévoit :

« *Conformément aux dispositions du deuxième alinéa de l'article 40 du code de procédure pénale, le maire est tenu de signaler sans délai au procureur de la République les crimes ou les délits dont il acquiert la connaissance dans l'exercice de ses fonctions*. »

b. Obligation de mise en place d'une procédure de recueil et protection des signalements d'alerte

La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique encadre la notion d'alerte en apportant une définition du « lanceur d'alerte », les modalités de sa protection et de la mise en place d'une procédure de recueil d'information d'alerte.

Ainsi, l'article 6 de cette même loi définit le lanceur d'alerte comme « *une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général, dont elle a eu personnellement connaissance* ».

Les articles 8 et 17 de cette même loi imposent la mise en place d'une procédure de recueil d'information d'alerte selon certains critères.

Sont concernés par ce dispositif :

- les communes de plus de 10 000 habitants ;
- les établissements publics de coopération intercommunale à fiscalité propre dont elles sont membres ;
- les départements ;
- les régions.

[106] Cet article est créé par l'ordonnance n°2012-351 du 12 mars 2012

Toutes ces instances doivent se doter d'un « dispositif d'alerte interne destiné à permettre le recueil des signalements émanant d'employés et relatifs à l'existence de conduite ou de situations contraires au code de conduite de la société ». En outre, cet article suppose la mise en place d'un code de conduite interne aux organisations citées ci-dessus (cf. annexe recommandations AFA)

Pour compléter ce dispositif d'alerte, l'article 9 encadre les obligations de protection des lanceurs d'alerte sous peine de deux ans d'emprisonnement et de 30 000€ d'amende en cas de non-respect[107].

La procédure de recueil d'alerte permet de garantir une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par le signalement et des informations recueillies.

Les éléments qui permettraient d'identifier le lanceur d'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire avec consentement de celui-ci.

Les éléments qui permettraient d'identifier la ou les personnes mises en cause ne peuvent être divulgués, sauf à l'autorité judiciaire et une fois le caractère fondé de l'alerte établi.

Les modalités d'exercice du lancement d'alerte (*Employee's whistleblowing right*) ont été fixées en dernier lieu dans les articles 6 à 16 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi « Sapin 2 ».

Ce droit nouveau dédié à la lutte contre la fraude donne lieu à la mise en place de mesures spécifiques de protection qui visent à prémunir les auteurs des lancements d'alerte d'éventuelles sanctions ou pressions propres à décourager leur initiative.

L'article 8-I prévoit ainsi le signalement de toute alerte « *est porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci* ». Hors les cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles, l'autorité en charge du droit du recueil des signalements d'alerte en vérifie la recevabilité et le bien-fondé « *dans un délai raisonnable* » ; dans le cas où elle manquerait à cette obligation les signalements seront adressés *« à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels* » et pourront être rendus publics en dernier ressort, à défaut de traitement par l'un ou l'autre de ces organismes.

L'article 8-III stipule que le droit de lancement d'alerte est organisé au travers de « *procédures appropriées de recueil des signalements émis par les membres [du] personnel ou par des collaborateurs extérieurs et occasionnels* ».

L'article 9 ajoute que ces procédures « *garantissent une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement* ».

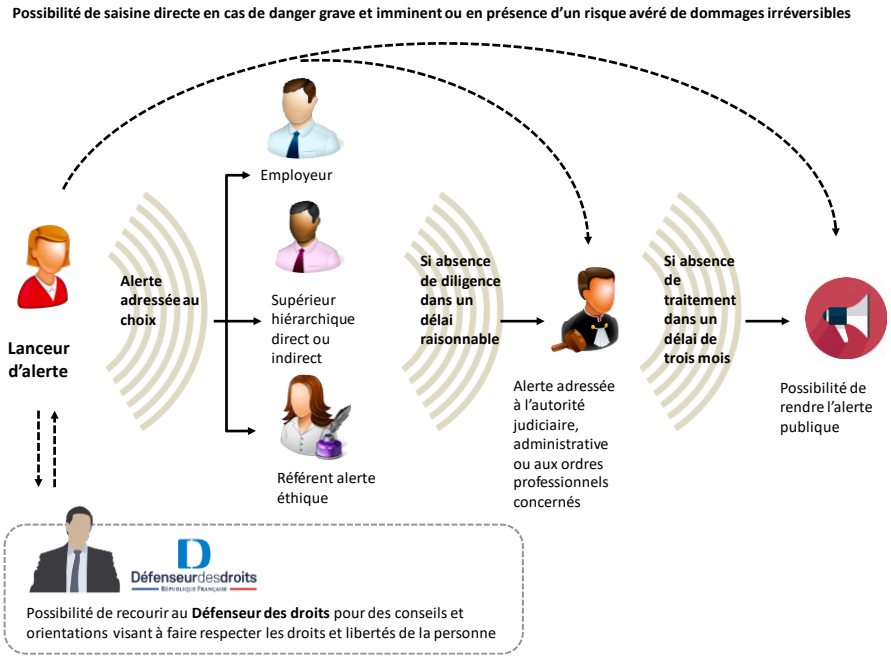
Le cadre de mise en œuvre du dispositif ainsi décrit est précisé dans le décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat qui est entré en vigueur le 1er janvier 2018.

Ce décret indique notamment que le référent mentionné à l'article 8-I de la loi peut être extérieur à l'organisme et dans tous les cas « *dispose, par son positionnement, de la compétence, de l'autorité et des moyens suffisants à l'exercice de ses missions* » (article 4).

Son article 5 mentionne également les informations fournies en accompagnement du recueil des signalements afin d'en garantir un bon et complet usage.

[107] Ces obligations se retrouvent également dans l'article L.135-2 du Code général de la fonction publique

Circuit-type de recueil et traitement d'un signalement d'alerte[108]



III. Obligation faite aux collectivités de mettre en œuvre un plan d'action pour la détection et la prévention des actes contraires à la probité sous le contrôle de l'Agence française anti-corruption (AFA)

La loi n° 2016-1691 du 9 décembre 2016 du 9 décembre 2016 crée une Agence française anti-corruption (AFA) sous la forme d'un service à compétence nationale placé auprès du ministre de la justice et du ministre chargé du budget, et lui assigne pour mission d'aider les acteurs privés et publics à prévenir et à détecter tout acte contraire à la probité qui serait susceptible d'affecter leur activité.

A cet effet et sur le fondement de l'article 3-2 de la loi, l'AFA émet des recommandations à l'usage de chaque catégorie d'acteurs afin de les aider à sécuriser leurs procédures et pratiques dans le sens attendu.

De même, l'article 3-3 prévoit que l'AFA « *contrôle, de sa propre initiative, la qualité et l'efficacité des procédures mises en œuvre au sein des administrations de l'Etat, des collectivités territoriales, de leurs établissements publics et sociétés d'économie mixte, et des associations et fondations reconnues d'utilité publique pour prévenir et détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme* ».

[108] Source : Guide pour la mise en œuvre par les collectivités territoriales des recommandations de l'Agence française anticorruption - Publication commune IFACI-CIAT (2019)

Pour effectuer ses contrôles, l'AFA s'assure de la bonne mise en place des recommandations qu'elle a édictée. Ces recommandations ne créent pas d'obligations juridiques auprès des collectivités territoriales mais accordent à celles qui les appliquent une présomption simple de conformité. Les collectivités qui choisissent un autre dispositif de lutte contre la corruption doivent justifier de son efficacité auprès des contrôles de l'AFA. Les collectivités territoriales sont donc fortement incitées à mettre en œuvre les dispositions de l'AFA.

Ainsi, les collectivités territoriales - en plus de leur obligation de mettre en œuvre les obligations réglementaires qui leur sont applicables (voir supra, Point II) - sont appelées à mettre en œuvre un plan d'action pour la prévention et la détection des actes contraires à la probité répondant aux recommandations en vigueur de l'AFA.

> Voir dans la **Fiche technique 4** le détail des recommandations de l'AFA à destination des collectivités territoriales

Fiche technique 1 > Annexe 1

Dispositions relatives à la transparence des actes et décisions

Obligation	Institutions concernées	Textes règlementaires de référence
Droit à communication des documents administratifs	Droit ouvert aux administrés	Art. L.311-1 du Code des relations entre le public et l'administration : *« les administrations […] sont tenues de publier en ligne ou de communiquer les documents administratifs qu'elles détiennent aux personnes qui en font la demande »*
Ouverture des données publiques	▪ Régions et Départements ▪ Communes comptant plus de 3 500 habitants ▪ Personnes morales de droit public comptant plus de 50 agents ▪ Personnes morales de droit privé chargées d'une mission de service public comptant plus de 50 salariés	Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
Tenue d'un répertoire/recueil des actes administratifs	▪ Régions et Départements ▪ Communes et EPCI comptant plus de 3 500 habitants (pour le recueil)	Art. R2121-10, 3131-1, 4141-1 et 5211-41 du Code des relations du public avec l'administration
Nomination d'un référent CADA[109]	▪ Régions et Départements ▪ Etablissements publics locaux comptant plus de 200 agents ▪ Communes et EPCI comptant plus de 10 000 habitants	Art. R.330-2 du Code des relations du public avec l'administration

[109] Responsable de l'accès aux documents administratifs et des questions relatives à la réutilisation des informations publiques

Fiche technique 1 > Annexe 2

Dispositions relatives à la prévention des conflits d'intérêts

Obligation	Qui ?	Institutions concernées	Textes règlementaires de référence
Encadrement des recrutements familiaux dans les cabinets[110]	L'autorité territoriale	▪ Régions, Départements, communes, et EPCI ▪ Obligations renforcées pour les communes et EPCI comptant respectivement plus de 20 000 habitants et 100 000 habitants	Article L.333- 1 à 6 du Code général de la fonction publique[111]
Déclarations d'intérêts et de situation patrimoniale	Exécutif et collaborateurs (directeurs, directeurs adjoints et chefs de cabinet)	▪ Régions et Département ▪ Communes et EPCI comptant plus de 20 000 habitants ▪ Obligations renforcées pour les communes et EPCI comptant plus de 100 000 habitants	Art. 11 de la loi n° 2013-907 du 11 octobre 2013 modifiée
Déclaration préalable d'intérêts	Emplois dont le niveau hiérarchique ou la nature des fonctions le justifient	▪ Régions et Départements ▪ Communes, EPCI, centres de gestion comptant plus de 80 000 habitants	Article L 122-2 à 122-25 du Code général de la fonction publique[112]
Déclaration de situation patrimoniale	Emplois dont le niveau hiérarchique ou la nature des fonctions le justifient	▪ Régions, Départements, communes, EPCI, syndicats mixtes, métropole d'Aix, CNFPT, CIG grande et petite couronne ▪ Centres de gestion comptant plus de 20 000 habitants ▪ Obligations renforcées pour les communes, EPCI, syndicats mixtes, centres de gestion, caisses de crédit municipal comptant plus de 150 000 habitants	Article L 122-10 du Code général de la fonction publique[113]

…/…

[110] En dehors d'un cabinet, l'autorité territoriale peut engager un membre de sa famille sous réserve de l'interdiction de toute prise illégale d'intérêt. En pareille circonstance, l'autorité territoriale doit exercer son obligation de déport et s'abstenir de tout acte relatif à l'embauche de cette personne.

[111] Anciennement article 110 de la loi n° 84-53 du 26 janvier 1984 modifiée

[112] Anciennement articles 25 ter et nonies de la loi n° 83-634 du 13 juillet 1983 modifiée

[113] Anciennement article 25 quinquies de la loi n°83-634 du13 juillet 1983 modifiée

Obligation	Qui ?	Institutions concernées	Textes règlementaires de référence
Obligation de déport des élus et des agents	Exécutifs territoriaux et leurs délégataires Tous les autres élus et les agents territoriaux	Régions, départements, communes, Etablissements publics de coopération intercommunale (EPCI)	Pour les élus : en application du décret n°2014-90 du 31 janvier 2014 pris en application de l'article 2 de la loi n°2013-907 du 11 octobre 2013 Pour les agents : en application de l'article L 122-1 du Code général de la fonction publique[114]

[114] Anciennement article 25 [bis] de la loi 83-634 du 13 juillet 1983

Fiche technique 2

Recommandations de l'Agence française anti-corruption relatives à la prévention et à la détection des actes contraires à la probité

L'article 3-2 de la loi n° 2016-1691 du 9 décembre 2016 dite « Loi Sapin 2 » dispose que l'Agence française anti-corruption (AFA) publie des recommandations à l'usage des acteurs privés et publics pour la mise en œuvre de dispositifs de détection et de prévention des actes contraires à la probité.

L'AFA a ainsi publié un premier ensemble de recommandations en décembre 2017[115] puis a procédé à sa mise à jour au travers d'un nouveau texte paru au JORF du 12 janvier 2021.

Ce texte contient les lignes directrices pour les collectivités territoriales.

Il couvre l'ensemble des actes contraires à la probité susceptible d'affecter le fonctionnement des collectivités territoriales.

> Voir **Annexe 1** - Actes contraires à la probité au sens de l'AFA

Les recommandations de l'AFA se présentent comme un mode opératoire pour la mise en œuvre de plans anti-corruption répondant à une architecture commune et par ailleurs largement adaptables aux moyens et besoins de chaque collectivité.

Cette architecture commune repose sur trois piliers :

Le premier pilier est relatif à **l'engagement de l'instance dirigeante** :

> Un engagement ferme et réfléchi de l'instance dirigeante conditionne la mise en œuvre réussie d'une politique de conformité anti-corruption. L'engagement de l'instance dirigeante doit se traduire par l'affirmation d'une volonté d'exemplarité, la mise en place d'un calendrier précis, la mobilisation des moyens humains et financiers nécessaires à la conduite du projet.

Le second pilier a trait à la réalisation d'une **cartographie des risques** d'atteinte à la probité au sein de la collectivité :

> Une cartographie des risques permet d'orienter les dispositifs de contrôle et les mesures de maîtrise sur les activités reconnues comme vulnérables car on ne saurait prévenir que ce que l'on a préalablement identifié et quantifié.

[115] Voir le JORF du 22 décembre 2017

Le troisième pilier regroupe l'ensemble des types de **mesures de préservation** de nature à contenir le risque de fraude :

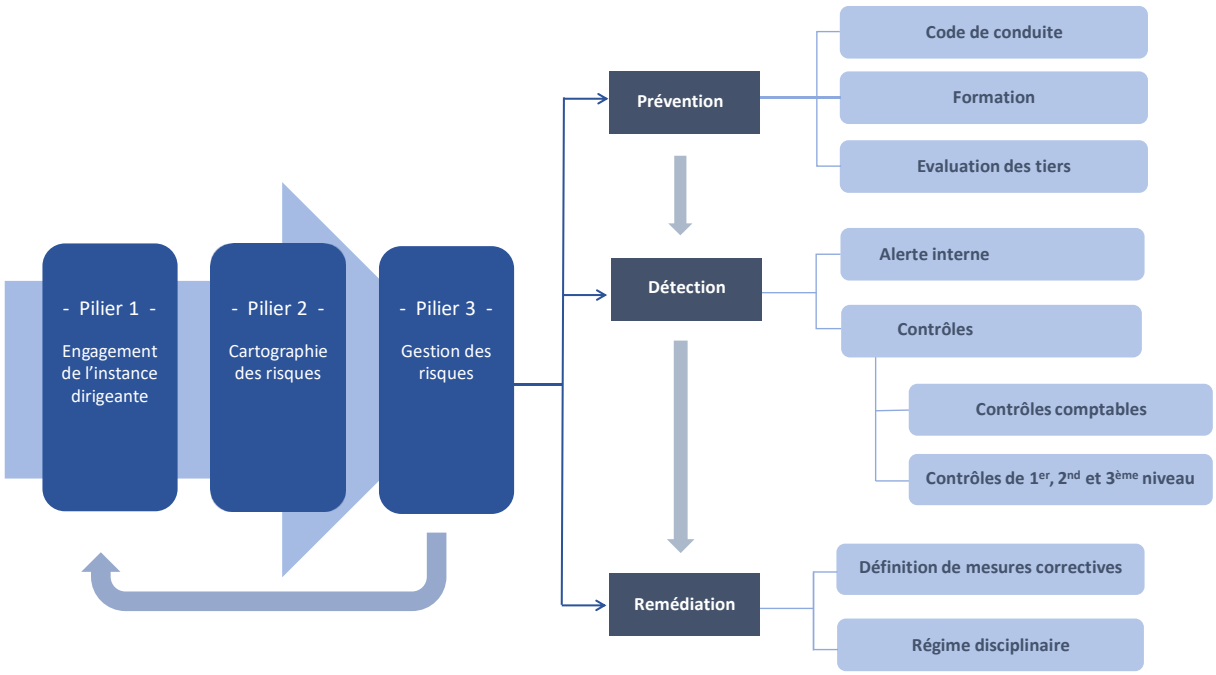
Les dispositifs constitutifs de ce dernier pilier devront :

- Revêtir un caractère préventif (mise en place d'un code de conduite, formation, évaluation des tiers) ;
- Prendre la forme de moyens de détection (alerte interne, contrôles comptables, contrôles internes de premier, second et troisième niveau) ;
- Être utilisés à des fins de remédiation (mesures correctives, sanctions disciplinaires et/ou pénales).

Cette approche opérationnelle et managériale s'adresse aux décideurs territoriaux et vise à faciliter l'appropriation collective de cette thématique complexe.

En plus de donner plus de lisibilité au cheminement méthodologique conduisant à la mise en place d'un plan anti-corruption robuste et pérenne, les recommandations actualisées renforcent sensiblement les conditions et modalités d'exercice d'opérations précédemment décrites.

Représentation graphique d'un dispositif de lutte anti-fraude au sens de l'AFA[116]



[116] Source : Recommandations de l'AFA parues au JORF du 12 janvier 2021

Engagement de l'instance dirigeante dans la mise en œuvre d'un dispositif anticorruption

Il est recommandé aux responsables des organisations du secteur public de s'engager publiquement en actes et en paroles en faveur d'une « *politique de tolérance zéro envers tout comportement contraire à l'intégrité et à la probité*[117] ».

A cet égard il leur est demandé :

- de faire preuve d'exemplarité ;
- d'encourager et valoriser dans leurs équipes les comportements éthiques ;
- de faire de la prévention et de la détection de la corruption une priorité explicite de l'organisation ;
- de montrer de la vigilance et du discernement dans la détection de tout comportement apparemment suspect ;
- de faire un usage réel et proportionné des possibilités des sanctions disciplinaires prévues par le statut général de la fonction publique et/ou le Code du travail.

Dans le cas où des indices de corruption sont relevés, les responsables hiérarchiques peuvent être amenés à prendre sans délai des mesures conservatoires telles que le retrait de certains dossiers en cours de traitement ou clos, l'interdiction de l'accès aux dossiers, la sécurisation de l'accès aux bureaux, aux notes et rapports ayant trait aux affaires du service ou aux moyens de travail et le cas échéant, le signalement des cas à la juridiction pénale[118].

Mise en place d'un code de conduite

Il est recommandé de mettre en place un code de conduite fixant les règles opposables aux agents et dont le non-respect est passible de sanctions disciplinaires et éventuellement de poursuites judiciaires.

Ce document porte en particulier sur les points suivants :

- rappel des raisons qui doivent conduire les acteurs publics à prévenir la corruption[119] ;
- présentation d'exemples de situations à risques de corruption et précise les moyens de gérer ces situations de manière adéquate ;
- définition du risque de conflit d'intérêts et organisation du déport dans les cas recensés[120] ;
- organisation de la déclaration obligatoire par les élus, les agents des conflits d'intérêts ;
- identification des conditions d'exercice conjoint d'un mandat électif et de fonctions administratives.

[117] En référence à l'article L 124-1 du Code général de la fonction publique (anciennement article 25 de la loi n° 83-634 du 13 juillet 1983 issu de l'article 1er de la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires) qui dispose : « Il appartient à tout chef de service de veiller au respect de ces principes [impartialité, intégrité, probité et neutralité] dans les services placés sous son autorité. Tout chef de service peut préciser, après avis des représentants du personnel, les principes déontologiques applicables aux agents placés sous son autorité, en les adaptant aux missions du service ».

[118] Notamment sur le fondement des dispositions de l'article 40 du Code pénal

[119] Il s'agit notamment de prévenir les atteintes à l'image de la collectivité, d'éventuels préjudices à ses intérêts moraux et financiers via une détérioration du service par la fourniture de biens, travaux et services non conformes ; une allocation sous-optimale des ressources ou encore de prévenir les atteintes à l'égalité de traitement entre administrés…

[120] Dossier engageant les intérêts de l'agent, de sa famille ou de son réseau amical

Son objet est de faciliter l'application des principes déontologiques dans la pratique quotidienne et de fixer les règles de comportement face aux situations concrètes rencontrées par les acteurs locaux.

Les informations données doivent être précises et adaptées aux risques identifiés dans le cadre de la cartographie des risques (voir ci-après le point 3).

En principe, le code de conduite ne se confond ni avec des chartes déontologiques conçues pour réaffirmer des principes généraux ni avec la Charte de l'Elu local créée par l'article 2 de la loi n° 2015-366 du 31 mars 2015 visant à faciliter l'exercice de leur mandat et codifiée dans un article L. 1111-1-1 du code général des collectivités territoriales.

Cependant, il apparaît que dans de nombreuses collectivités territoriales les guides de déontologie, applicable aux élus et/ou aux agents, ou les chartes de déontologie, font office de code de conduite, en y introduisant des exemples concrets ou illustrations.

Cette situation correspond à une étape tout à fait acceptable dans un cheminement vers une appropriation étendue de ces questions ; il importe dans tous les cas que les exemples et illustrations apportés soient concrets et pragmatiques, de manière à illustrer efficacement les valeurs et les principes déontologiques portés par la collectivité.

Mise en place d'une cartographie des risques de corruption

Il est recommandé de mettre en place une cartographie des risques de corruption[121] dans le but d'identifier, évaluer et hiérarchiser les risques de corruption inhérents aux compétences, aux activités et aux processus de l'organisation et de de mettre en place les moyens de maitrise les mieux appropriés.

Son élaboration doit engager l'ensemble de la chaîne hiérarchique et le cas échéant les élus.

L'ensemble des étapes des processus de décision ou d'action doit être précisément étudié afin que soit prise en considération toute situation dans laquelle un agent public dans le cadre du service ou un élu est susceptible d'octroyer, solliciter ou recevoir un avantage indu ou d'en accepter la promesse, que ce soit en contrepartie d'une décision ou en cas d'abstention à prendre une décision.

La cartographie des risques de fraude prend également appui sur des faits ou des indices recensés.

Le fait que des indices ou des faits de corruption aient été détectés doit conduire à consigner ces indices ou faits ainsi que leurs circonstances de déclenchement et des mesures correctives prises, de manière à en assurer la traçabilité[122].

La cartographie des risques de fraude peut notamment conduire à la mise en œuvre de mesures préventives ciblées telles que :

- la sécurisation des procédures ;
- le renforcement du contrôle interne ;
- le changement d'affectation de certains agents ou responsables, nommés ou élus ;
- la rationalisation des droits d'accès aux systèmes d'information ;
- la vérification de l'intégrité des cocontractants et partenaires ;
- le renforcement du contrôle de la passation et de l'exécution des marchés ;
- le renforcement du contrôle de l'octroi et de l'utilisation des subventions.

[121] Le terme « corruption » recouvre ici les 6 types de délits mentionnés dans l'Annexe 1 de la présente Fiche technique

[122] La conservation de ces éléments doit être assurée en toute confidentialité à moins que des sanctions disciplinaires aient été prises pour ce motif à l'encontre du ou des agent(s) ou élu(s) concernés et sans préjudice des obligations de signalement issues de l'article 40 du Code pénal

La cartographie des risques de fraude doit être révisée régulièrement et actualisée aussi souvent que nécessaire pour tenir compte de l'évolution du périmètre des compétences et des procédures.

> Voir **Annexe 2** - Exemple de scénarios de risques pour les acteurs publics

Mise en place d'un dispositif d'alerte interne

Le décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat prévoit l'activation de ce dispositif à compter du 1er janvier 2018.

Il est recommandé de donner à l'ouverture de ce nouveau droit une publicité adéquate afin que l'ensemble des agents et acteurs concernés soient complétement informés des circonstances et des modalités de recueil des signalements, des garanties de confidentialité données ainsi que des suites qu'ils peuvent en attendre.

La diffusion de ces éléments peut être notamment assurée par voie de notification, affichage ou publication et le cas échéant sur leur site internet de l'organisme.

Les collaborateurs extérieurs et occasionnels des administrations et collectivités doivent avoir accès aux mêmes informations.

Mise en place d'une procédure d'évaluation des tiers

Il est recommandé de mettre en place une procédure d'évaluation des tiers, en donnant à la notion de « tiers » la notion extensive de tout partenaire extérieur de l'organisme[123].

Les procédures d'évaluation des tiers se traduisent par la mise en œuvre de vérifications consistant à évaluer le risque spécifique induit par la relation établie ou envisagée avec un tiers donné.

Cet exercice est conduit sur la base de la cartographie des risques (point 3).

Ce dispositif d'évaluation interne doit excéder les diligences particulières prévues par les lois et règlements[124].

Il peut également amener les acheteurs publics à introduire des préconisations ou des prescriptions anticorruptions dans le cahier des charges des engagements qu'ils souscrivent de manière à favoriser un comportement intègre des parties en amont de l'engagement et dans le cadre de son exécution.

[123] Soit en particulier des candidats à l'attribution de marchés ou des titulaires de marchés, des organismes sollicitant ou obtenant des subventions, des candidats à un recrutement, des candidats à l'acquisition de biens, des occupants et candidats à l'occupation d'un domaine public

[124] Dans le domaine de la commande publique, l'ordonnance n° 2015-899 du 23 juillet 2015 prévoit ainsi de vérifier si les candidats ne sont pas sous le coup d'une mesure d'exclusion de la procédure de passation des marchés publics, en raison d'une condamnation définitive (articles 45 et 46)

Mise en place de dispositifs de contrôle et d'évaluation interne

Il est recommandé de mettre en place des dispositifs de contrôle et d'évaluation interne dédiés à la prévention des risques de corruption.

Ces dispositifs ont vocation à appréhender l'ensemble des activités porteuses d'aléas en matière de probité, en interne comme dans les relations avec les organismes périphériques et avec les tiers, en tenant compte des points d'attention prioritaires fixés par la cartographie des risques (point 3).

Les investigations menées répondent aux quatre objectifs suivants :

- Contrôler la mise en œuvre des mesures de prévention et de détection de la corruption et tester leur efficacité ;
- Identifier et mesurer d'éventuels manquements dans l'exécution des procédures ;
- Définir des recommandations ou autres mesures correctives adaptées, si nécessaire, en vue d'améliorer l'efficacité du programme de conformité anticorruption ;
- Détecter, le cas échéant, des faits de corruption.

Les contrôles et évaluations internes visent à vérifier que le dispositif mis en place est opérationnel et adapté au risque de corruption ; ils permettent également de repérer tout dysfonctionnement et susciter en réponse les mesures correctives requises.

Renforcement de la procédure de contrôle comptable

Dans le prolongement de la précédente recommandation, il est proposé de mettre en œuvre des procédures de contrôles comptables, internes ou externes, destinées à s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de corruption ou de trafic d'influence.

Il ne s'agit pas de créer de procédures comptables spécifiques mais de mesurer le risque intrinsèque lié à une rigueur comptable insuffisante.

Il convient d'effectuer ce contrôle sur trois niveaux :

- contrôle de premier niveau auprès des personnes en charge de la saisie et de la validation des écritures comptables, en s'assurant en particulier de la séparation des tâches et de système de validation indépendants ou croisés ;
- contrôle de deuxième niveau qui vise à établir une cartographie des risques et à garantir la maturité et le bon fonctionnement des contrôles de premier niveau ;
- contrôle de troisième niveau à travers des audits internes ou externes sur l'ensemble des dispositifs comptables, en particulier la prise en compte du risque de corruption au sein de la collectivité.

Mise en place d'un dispositif de formation aux risques de corruption

Il est enfin recommandé de mettre en place un dispositif global de formation aux risques de corruption afin de proposer des contenus différenciés à certains publics prioritaires :

- Les agents occupant les fonctions et les mandats les plus exposés aux risques de corruption ;
- Les agents occupant des fonctions d'encadrement ou d'audit ou de contrôle ;
- Les agents nouvellement recrutés ou aux nouveaux élus.

L'identification des fonctions et des mandats les plus exposés est réalisée sur la base de la cartographie des risques (point 3).

Le plan de formation doit toutefois s'étendre à l'ensemble des agents en relation avec des tiers.

Il convient à cet effet d'utiliser l'ensemble des supports de formation existants (formations présentielles, documentation pédagogique) et de rechercher des partenariats avec les organismes de formation agréés, les associations professionnelles et les établissements du Réseau des écoles de service public proposant des modules sur cette thématique.

Fiche technique 2 > Annexe 1

Actes contraires à probité au sens de l'AFA

Délit	Textes réglementaires	Définition
Corruption	Articles 432-11 et s, 433-1 1° et s, 434-9 et s, 435-1 et s, 445-1 et s du Code pénal	La corruption est une infraction ancienne (déjà visée dans le code pénal de 1810), qui a longtemps été unique dans la catégorie des manquements au devoir de probité, avant l'ajout du trafic d'influence à la fin du XIXe siècle. Elle vise le comportement par lequel sont sollicités, acceptés, reçus des offres, promesses, dons ou présents proposés à des fins d'accomplissement ou d'abstention d'un acte, d'obtention de faveurs ou d'avantages particuliers. L'infraction n'a cessé au fil des années, de voir son champ d'application étendu : fonctionnaires, agents publics étrangers, élus, mais aussi personnes travaillant dans le secteur privé. La corruption active et la corruption passive sont deux infractions complémentaires mais autonomes Les agissements du corrupteur *(corruption active)* et ceux du corrompu *(corruption passive)* peuvent être poursuivis et jugés séparément et la répression de l'un n'est nullement subordonnée à la sanction de l'autre. En fait, le corrompu accepte des promesses, des présents des dons et peut même les solliciter alors que le corrupteur offre des présents et des dons, fait des promesses jusqu'à céder aux sollicitations du corrompu en lui remettant l'objet de la corruption.
Concussion	Article 432-10 et s du Code pénal	La concussion est une infraction commise par un représentant de l'autorité publique ou une personne chargée d'une mission de service public qui, sciemment, reçoit, exige ou ordonne de percevoir une somme qui n'est pas due. C'est aussi le cas lorsque ce représentant ou cette personne accorde, sous une forme quelconque et pour quelque motif que ce soit, une exonération ou franchise des droits, contributions, impôts ou taxes publics en violation des textes légaux ou réglementaires. Sont visées par l'infraction de concussion, les personnes dépositaires de l'autorité publique ou chargées d'une mission de service public. La concussion entre dans la catégorie des infractions de commission qui nécessitent, pour être consommées, que l'auteur ait agi positivement et ne se soit pas contenté de s'abstenir d'agir.

Délit	Textes règlementaires	Définition
Prise illégale d'intérêts	Article 432-12 et s du Code pénal [125]	Ce délit est le fait pour une personne dépositaire de l'autorité publique, chargée d'une mission de service public ou investie d'un mandat électif public, d'avoir pris, reçu ou conservé directement ou indirectement, un intérêt de nature à compromettre son impartialité, son indépendance ou son objectivité dans une entreprise ou dans une opération dont il avait, au moment de l'acte, en tout ou en partie, la charge d'assurer soit la surveillance ou l'administration, soit la liquidation ou le paiement. La prise illégale d'intérêts doit être distinguée du simple conflit d'intérêts qui est une situation de fait mais ne constitue pas en soi un délit. Le seul conflit est un risque. Ce dernier constitue la remise en cause potentielle de la neutralité et de l'impartialité avec lesquelles l'agent public doit accomplir sa mission du fait de ses intérêts personnels. Le conflit entre ces intérêts contradictoires est simplement une situation d'exposition au risque qui peut, si les intérêts sont confondus, devenir une prise illégale d'intérêt...
Détournement de fonds publics	Articles 432-15 et 433- 4 du Code pénal	Le détournement de fonds publics est visé par l'infraction de détournement de biens publics effectué soit par une personne chargée d'une fonction publique, soit par un particulier. Le détournement ou la soustraction de biens publics par une personne chargée d'une fonction publique est le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, un comptable public, un dépositaire public ou l'un de ses subordonnés, de détruire, détourner, soustraire ou tenter de détruire, détourner ou soustraire, un acte ou un titre, des fonds publics ou privés, des effets, pièces ou titres en tenant lieu, ou tout autre objet qui lui avaient été remis en raison de sa fonction ou de sa mission.

[125] L'infraction de prise illégale d'intérêts a été définie en dernier lieu par l'article 15 de la loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire

Délit	Textes règlementaires	Définition
Favoritisme	**Article 432-14 et s du Code pénal**	Le favoritisme est une infraction plus récente (1991) ayant pour but de moraliser l'attribution des marchés publics et des délégations de service public. Le délit de favoritisme protège l'impératif de probité des élus et agents publics tout en assurant le respect des grands principes de la commande publique (liberté d'accès à la commande publique, égalité de traitement, transparence ces procédures). Ce délit recouvre la plus large catégorie d'auteurs puisqu'il concerne aussi bien les élus et agents publics que les personnes privées intervenant dans la procédure d'attribution d'un marché public, à quelque stade que ce soit, ainsi que les mandataires des personnes susmentionnées. Le favoritisme est le fait par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ou investi d'un mandat électif public ou exerçant les fonctions de représentant, administrateur ou agent de l'État, des collectivités territoriales, des établissements publics, des sociétés d'économie mixte d'intérêt national chargées d'une mission de service public et des sociétés d'économie mixte d'intérêt local de procurer ou de tenter de procurer à autrui un avantage injustifié par un acte contraire aux dispositions législatives ou règlementaires ayant pour objet de garantir la liberté d'accès et l'égalité des candidats dans les marchés publics et les contrats de concession. Pour que l'infraction de favoritisme soit constituée, il est nécessaire qu'un texte précis du Code de la commande publique ou du Code général des collectivités territoriales régissant les marchés publics ait été violé. C'est une infraction formelle qui prévient la commission d'atteinte à la probité plus graves et souvent plus difficiles à caractériser, tel que le délit de corruption qui trouverait pour support la conclusion d'un marché public.

Fiche technique 2 > Annexe 2

Exemple de scénarios de risques de fraude pour les acteurs publics

L'AFA préconise la mise en place d'une cartographie des risques de fraude à l'échelle de chaque collectivité permettant de positionner et dimensionner les mesures de détection et prévention reconnues comme nécessaires.

Dans l'annexe n° 2 de sa recommandation du 12 janvier 2021, l'AFA a ainsi identifié des exemples de scénarios de risques dans les trois processus suivants de gestion publique :

- Le versement de subventions ;
- La gestion des ressources humaines ;
- La commande publique.

En réponse, elle propose des mesures de prévention et de détection ainsi que des bonnes pratiques de nature à atténuer ces risques.

L'AFA suggère aux collectivités qui ne seraient pas familiarisées avec une démarche de management des risques d'examiner prioritairement ces processus de gestion publique au démarrage de leurs travaux de cartographie.

Recommandations de l'AFA destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêts, de détournement de fonds publics et de favoritisme publiées aux JORF du 12 janvier 2021

Paragraphe 410 - « *Les acteurs publics pas ou peu familiers des exercices de cartographie des risques peuvent utilement, dans leur cheminement tendant à se doter d'une cartographie des risques d'atteintes à la probité, telle que proposée dans les précédents paragraphes, débuter leurs travaux en examinant prioritairement trois processus que l'expérience conduit à considérer comme particulièrement exposés aux risques d'atteintes à la probité : la commande publique, la gestion des ressources humaines, le versement des subventions (cf. annexe n° 2).* »

Les exemples donnés ci-après ne sont pas exhaustifs ; ils ont vocation à être adaptés et complétés en fonction du profil de risque de chaque collectivité.

a) Traitement des risques de fraude associés au versement de subventions

Type de fraude (voir Annexe 1)	Illustrations (exemples)	Mesures préventives recommandées
Détournement de fonds publics	▪ Attribution d'une subvention à un organisme écran ▪ Versement d'une subvention alors que le dossier de demande est incomplet. ▪ Versement des fonds publics non pas à l'organisme demandeur, mais à un tiers qui a substitué son identité bancaire à celle de l'association. ▪ L'organisme bénéficiaire affecte tout ou partie des fonds publics reçus à un usage autre que celui qui a justifié le versement de la subvention.	▪ Sensibiliser et former les agents publics et les élus à la question des conflits d'intérêts et aux réponses appropriées (déport…) ▪ Etablir le dossier de demande de subvention de manière à pouvoir vérifier l'existence de l'organisme demandeur, la réalité de son activité et l'identité des personnes participant à sa gouvernance ▪ Réaliser des études de notoriété des organismes demandeurs ▪ Réaliser des contrôles de cohérence systématiques entre l'identité de l'organisme attributaire de la subvention et l'identité du titulaire du compte bancaire sur lequel les fonds seront versés. ▪ Prévoir une obligation conventionnelle de rendre compte de l'usage de la subvention attribuée. ▪ Conditionner le versement de la totalité ou tout du moins du solde de la subvention à la production d'un compte rendu de gestion, demander des justificatifs des actions menées, réaliser des visites sur place. ▪ Mettre en place un contrôle (éventuellement par sondage) des modalités d'instruction des dossiers de demande de financement
Prise illégale d'intérêts	▪ L'instruction du dossier est réalisée par un agent public qui a un intérêt personnel à ce que la subvention soit ou non attribuée ▪ Une personne appelée à décider de l'attribution de la subvention individuellement ou dans un cadre collégial a un intérêt à ce que la subvention soit ou ne soit pas attribuée.	

b) Traitement des risques de fraude associés à la Gestion des ressources humaines

Type de fraude (voir Annexe 1)	Illustrations (exemples)	Mesures préventives recommandées
Corruption et trafic d'influence	▪ Un recrutement est décidé en contrepartie d'un avantage octroyé au recruteur ou à une personne qui exerce une influence sur le recruteur.	▪ Sensibiliser et former les agents à la gestion des conflits d'intérêts, pour autant que possible dès la phase de recrutements. ▪ Favoriser l'accès des agents au déontologue - voir article L 124-2 du Code général de la fonction publique[126] pour obtenir des éclairages en la matière. ▪ Rapprocher régulièrement les fiches de paie avec l'organigramme des services. ▪ Rechercher l'automatisation du calcul des avancements et reclassements dans le système d'information de gestion des ressources humaines et prévoir un contrôle hiérarchique en cas de forçage manuel. ▪ Sécuriser les modalités d'habilitation des agents habilités à intervenir sur les dossiers individuels RH ▪ Vérifier systématiquement les évolutions atypiques des montants de la paie des agents ▪ Procéder, à échéance régulière, à des contrôles par sondage des saisies ▪ Prévoir une rotation des agents occupant des postes particulièrement exposés aux atteintes à la probité.
Prise illégale d'intérêts	▪ Un recruteur ou un membre du jury de recrutement omet de déclarer qu'il a des liens personnels avec un candidat et participe au processus de décision concernant son embauche ou sa promotion.	
Détournement de fonds publics	▪ Suite à son recrutement, un agent est rémunéré mais ne travaille pas pour l'entité publique et occupe de ce fait un emploi fictif ▪ Un gestionnaire de carrière ou de paie crée un collaborateur fictif dans le système d'information de gestion des ressources humaines, lui associe son propre compte bancaire et perçoit, par ce biais, une rémunération liée à un emploi fictif.	
Concussion	▪ Un agent déclare des heures supplémentaires qu'il n'a pas effectuées pour toucher la rémunération associée. ▪ Un agent perçoit un traitement indiciaire indu après avoir délibérément fourni des éléments inexacts ayant conduit à une reconstitution de carrière à son avantage.	

[126] Anciennement article 11 de la loi n° 2016-483 du 20 avril 2016

c) Traitement des risques de fraude associés à la commande publique

Type de fraude (voir Annexe 1)	Illustrations (exemples)	Mesures préventives recommandées
Corruption	▪ Attribution d'un marché à un opérateur économique en contrepartie d'une somme qu'il verse au décideur (	<u>En amont de la consultation</u> ▪ Veiller au choix de la procédure de consultation prescrite au regard des seuils et de la nature de la commande ▪ Appliquer strictement les critères justifiant le recours à des procédures dérogatoires <u>En phase de consultation</u> ▪ Offrir le même niveau d'information à tous les candidats ▪ Justifier le choix des critères d'analyse des offres, notamment les critères techniques. <u>En phase d'attribution</u> ▪ Mettre en œuvre un déport systématique des décideurs ayant un intérêt (financier ou moral) dans l'attribution du marché ▪ Privilégier un choix collégial pour l'attribution des marchés à procédures adaptées. <u>En phase d'exécution</u> ▪ Porter une attention particulière au service fait, réaliser des contrôles réguliers sur les prestations ou travaux réellement réceptionnés (volume, qualité)
Trafic d'influence	▪ Attribution d'un marché à un opérateur économique en contrepartie d'une somme qu'on lui propose de verser pour influencer un décideur public	
Favoritisme	▪ Choix inadapté de la procédure de consultation. ▪ Recours non justifié aux procédures dérogatoires (urgence/marché négocié sans mise en concurrence). ▪ Traitement plus favorable d'une des organisations au cours de la consultation (communication d'informations privilégiées…) ▪ Choix de critères d'analyse des offres biaisé en faveur d'un candidat ou d'une catégorie de candidats	
Prise illégale d'intérêts	▪ Participation d'un élu à la commission d'appel d'offres alors qu'une des organisations candidates est détenue par un proche, même dans le cas où cette offre n'est pas retenue	
Détournement de fonds publics	▪ Paiement de prestations ou de travaux commandés, mais non réalisés ou partiellement réalisés. ▪ Établissement d'avenants dans des conditions contraires aux règles de la commande publique aux fins d'avantager le titulaire du marché.	

Fiche technique 3

Obligations liées à la mise en œuvre des financements de la politique européenne de cohésion

---

L'article 3 du traité sur l'Union européenne[127] dispose : « *L'Union (…) promeut la cohésion économique, sociale et territoriale, et la solidarité entre les États membres*. »

Cet objectif est mis en œuvre dans le cadre d'une politique de cohésion européenne mobilisant des financements dédiés, tels que mentionnés aux articles 174 à 178 du Traité de fonctionnement de l'Union européenne (TFUE) [128].

L'article 175 du TFUE énonce ainsi : « *L'Union soutient [le renforcement de sa cohésion économique, sociale et territoriale] par l'action qu'elle mène au travers des fonds à finalité structurelle (Fonds européen d'orientation et de garantie agricole, section «Orientation»; Fonds social européen ; Fonds européen de développement régional), de la Banque européenne d'investissement et des autres instruments financiers existants.* ».

De même, le point c) du second paragraphe de l'article 4 place la politique de cohésion au nombre des domaines de compétence partagée entre l'Union et les Etats-membres.

Les collectivités territoriales peuvent contribuer à l'utilisation des financements dédiés à la politique européenne de cohésion :

- Soit en tant qu'autorités de gestion, responsables en dernier ressort de la conduite d'un ou plusieurs programme(s) mono ou pluri-fonds, dans leurs ressorts géographiques et leurs domaines d'intervention respectifs[129] ;
- Soit en tant que délégataires de gestion (organismes intermédiaires) en charge de dispositifs concourant aux objectifs d'un programme, désignés à cet effet par l'autorité de gestion concernée et agissant sous la supervision et la responsabilité finale de cette dernière[130].

[127] Traité signé à Maastricht (1992) successivement modifié à Amsterdam (1997), Nice (2001) et Lisbonne (2009)

[128] Traité fondateur signé à Rome (1957) modifié à Lisbonne (2007)

[129] Depuis 2014, les Régions exercent les fonctions d'autorités de gestion des programmes du Fonds européen de développement régional et de la part du Fonds social européen abondant leurs politiques de formation ; elles ont en outre la responsabilité finale de la mise en œuvre des programmes du Fonds européen d'orientation et de garantie agricole. Parallèlement, l'Etat se réserve pour l'essentiel l'exécution d'un programme national du Fonds social européen dédié aux politiques de l'emploi et de l'inclusion.

[130] De nombreuses collectivités - notamment des Départements, des métropoles, des groupements de communes - sont associés en qualité d'organismes intermédiaires au déploiement de la politique européenne de cohésion, tout particulièrement dans le cadre du programme national du Fonds social européen dédié aux politiques d'emploi et d'inclusion.

Or, dans la mesure où elles se voient attribuer une responsabilité de gestion de financements européens dédiés à la politique de cohésion - et sans qu'il y ait lieu de distinction de fond à apporter entre autorités de gestion et organismes intermédiaires - les collectivités territoriales sont tenues de se conformer à un socle d'obligations générales et spécifiques constitué comme suit.

a) Un principe général de bonne gestion des financements de l'Union

Le règlement n° 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union (dit « règlement financier ») expose dans son article 33 que la mise en œuvre des fonds disponibles est régie par des principes d'économie, d'efficience et d'efficacité (*sound financial management*).

Différentes dispositions concourent à cet objectif.

En particulier, l'article 36 définit des modalités de contrôle interne attaché à l'exécution budgétaire, lesquelles comprennent « *la gestion appropriée des risques concernant la légalité et la régularité des opérations sous-jacentes, en tenant compte du caractère pluriannuel des programmes et de la nature des paiements concernés* » - cf. e) du second paragraphe.

De même, selon les termes de l'article 118 concernant les responsabilités et prérogatives de l'auditeur interne, celui-ci «*conseille son institution de l'Union dans la maîtrise des risques, en formulant des avis indépendants portant sur la qualité des systèmes de gestion et de contrôle et en émettant des recommandations pour améliorer les conditions d'exécution des opérations et promouvoir la bonne gestion financière.* »

L'article 63 relatif à la gestion partagée étend ces obligations aux organismes ayant part à la mise en œuvre des crédits de l'Union et désignés à cet effet par les Etats-membres.

Au a) du 4ème paragraphe, il est ainsi indiqué que ces organismes mettent en place un système de contrôle interne efficace et efficient (*effective and efficient internal control system*) et en assurent le fonctionnement.

Au b) du 5ème paragraphe il est précisé qu'ils fournissent à la Commission *« au plus tard le 15 février de l'exercice suivant (…) un résumé annuel des rapports finaux d'audit et des contrôles effectués, y compris une analyse de la nature et de l'étendue des erreurs et des faiblesses relevées dans les systèmes, ainsi que les mesures correctrices prises ou prévues* ».

b) Une attention particulière portée aux dispositifs de lutte anti-fraude

La lutte contre la fraude, la corruption et toute autre activité illégale est une pierre d'angle de la mise en œuvre des politiques de l'Union.

L'article 325 paragraphe 2 du Traité sur le fonctionnement de l'Union européenne (TFUE) indique ainsi que « *les États membres prennent les mêmes mesures pour combattre la fraude portant atteinte aux intérêts financiers de l'Union que celles qu'ils prennent pour combattre la fraude portant atteinte à leurs propres intérêts financiers*.»

Un organisme dédié à la détection et à la répression des actes de fraude susceptibles de porter atteinte aux intérêts financiers de l'Union a été créé sous le nom d'Office européen de lutte anti-fraude (OLAF)[131.]

Par ailleurs, cette thématique est largement reprise dans le règlement financier susmentionné.

Au point c) du second paragraphe de son article 36, il est indiqué que le Contrôle interne de l'exécution budgétaire vise spécifiquement à « *la prévention, [à] la détection, [à] la correction et [au] suivi de la fraude et des irrégularités* ».

En outre le point c) du second paragraphe de l'article 63 précise, que dans un cadre de gestion partagée, les États membres « *prennent toutes les mesures législatives, réglementaires et administratives qui sont nécessaires à la protection des intérêts financiers de l'Union [telles que] prévenir, détecter et corriger les irrégularités et la fraude* ».

Enfin le second paragraphe de l'article 91 relatif à la responsabilité des acteurs financiers pour activité illégale, fraude ou corruption prévoit « *les autorités et les instances désignées par la législation en vigueur* » saisissent l'OLAF de tout constat de cette nature.

La notion de fraude au sens des textes communautaires

Un acte de fraude repose sur une irrégularité, ainsi définie dans l'article 1 du règlement n° 2988/95 du 18 décembre 1995 relatif à la protection des intérêts financiers des Communautés européennes : «*toute violation d'une disposition du droit communautaire résultant d'un acte ou d'une omission d'un opérateur économique qui a ou aurait pour effet de porter préjudice au budget général des Communautés, ou à des budgets gérés par celles-ci, soit par la diminution ou la suppression de recettes provenant des ressources propres perçues directement pour le compte des Communautés, soit par une dépense indue*».

La Convention établie sur la base de l'article K.3 du Traité sur l'Union européenne (TUE) relative à la protection des intérêts financiers des Communautés européennes ajoute un caractère d'intentionnalité.

La fraude y est ainsi décrite comme « *tout acte ou omission intentionnel relatif à l'utilisation ou à la présentation de déclarations ou de documents faux, inexacts ou incomplets, ayant pour effet la perception ou la rétention indue de fonds provenant du budget général des Communautés européennes ou des budgets gérés par celles-ci ou pour leur compte; à la non-communication d'une information en violation d'une obligation spécifique, ayant le même effet ; au détournement de tels fonds à d'autres fins que celles pour lesquelles ils ont initialement été octroyés*.»[132]

131 Pour plus d'informations voir le Règlement (UE, Euratom) no 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF)

132 Voir JO C 316 du 27 novembre 1995

c) Un paquet réglementaire spécifique à chaque génération de programmes décline la mise en application de ces principes généraux

La politique européenne de cohésion est mise en œuvre dans le cadre de générations de programmes successives.

Ces générations de programmes couvrent des périodes pluriannuelles auxquelles sont attachés des objectifs stratégiques établis à l'échelle de l'Union, en matière de croissance inclusive et durable.

Un paquet réglementaire est publié au démarrage de chaque génération de programmes pour définir les modalités d'utilisation de ces fonds, en accord avec les principes fixés par le règlement financier applicable à l'exécution du budget de l'Union.

Les paquets réglementaires accompagnant les générations de programmes sont constitués :

- D'un règlement portant dispositions communes à l'ensemble des fonds de la politique européenne de cohésion (dit aussi « règlement général ») ;
- De règlements spécifiques à chaque fonds particulier ;
- De règlements délégués fixant le détail d'application des règlements susdits et plus particulièrement du règlement général.

Ces textes contiennent les prescriptions requises pour l'utilisation des crédits européens dans une perspective de bonne gestion financière, de lutte anti-fraude et de parfait rendu compte des actions cofinancées.

La génération de programmes comprise entre 2014 et 2020 est ainsi régie par le règlement général n° 1303-2013 publié le 17 décembre 2013 et modifié à plusieurs reprises depuis lors.

Les responsabilités respectives de la Commission européenne et des Etats membres dans le processus de sécurisation des systèmes de gestion et de contrôle des programmes de la politique européenne de cohésion de la période 2014-2020 sont notamment décrites dans les articles 72 à 75 et 122 de ce règlement.

Dans ce cadre général, une attention particulière doit être donnée à l'article 125 qui détermine les responsabilités des autorités de gestion désignées pour assurer la mise en œuvre des programmes.

En contrepoint, l'article 127 fixe les fonctions et prérogatives d'une Autorité d'audit chargée de l'évaluation de la qualité de gestion des programmes pour le compte de la Commission européenne et sous sa supervision finale.

Ce rôle est confié à la Commission interministérielle de coordination des contrôles (CICC).

En tant qu'autorité d'audit nationale, elle coordonne des campagnes annuelles d'audit d'opérations tout au long de la durée d'exécution des programmes afin de vérifier que les dépenses éligibles certifiées présentées aux instances communautaires pour remboursement de l'aide due ne sont pas affectés d'irrégularités dépassant un seuil de notification acceptable.

En complément et sur le fondement de l'article 75-2, la Commission européenne peut faire procéder à des audits ou contrôles sur place visant en particulier à « *la vérification du fonctionnement effectif des systèmes de gestion et de contrôle d'un programme ou d'une partie de programme, des opérations et […] l'évaluation de la bonne gestion financière des opérations et des programmes* ».

Dans le cas de manquement grave aux obligations incombant aux autorités de gestion, la Commission européenne peut être amenée à procéder à des corrections financières calculée proportionnellement au préjudice causé au budget de l'Union, selon une procédure fixée dans les articles 144 à 147 du règlement général n° 1303-2013 du 17 décembre 2013.

Ces corrections financières sont à la charge des autorités de gestion des programmes reconnues comme défaillantes, soit en particulier les Régions ; elles peuvent être répercutées auprès d'organismes intermédiaires s'il est établi que ceux-ci ont une part directe dans les dysfonctionnements constatés.

En dernier lieu, les autorités de gestion et/ou les organismes intermédiaires peuvent se retourner vers les maîtres d'ouvrage bénéficiaires de financements européens pour recouvrer tout ou partie du montant de leur correction financière appliquée à leur endroit, dans la mesure où ils ne portent pas l'entière responsabilité de cette situation.

Dans tous les cas, les collectivités prenant part à la mise en œuvre de programme de la politique européenne de cohésion bénéficient d'opportunités importantes du fait de la possibilité qui leur est donnée de mobiliser de nouveaux crédits en appui de leurs politiques ; en contrepartie elles s'exposent à des risques financiers, stratégiques et de réputation du fait des sanctions qui s'attachent à une mauvaise utilisation de ces financements.

En outre, toute collectivité candidate à la gestion de financements européens doit justifier d'une attention particulière en matière de détection et prévention des actes de fraude.

Dispositions particulières à la lutte anti-fraude (période 2014-2020)

En tant qu'autorités de gestion, les Régions sont tenues de mettre en place « *des mesures antifraude efficaces et proportionnées, tenant compte des risques identifiés* »[133].

En outre et selon les dispositions de l'article 122-2 du règlement général, elles ont l'obligation de signaler à la Commission européenne les irrégularités détectées de tout montant, en cas de soupçon de fraude[134].

La Commission européenne est également tenue informée des suites données (évolutions des procédures administratives et judiciaires, mesures prises en réponse à ce constat...).

Le signalement est réalisé au « *premier acte de constat administratif ou judiciaire*» défini dans le règlement délégué n° 2015-1970 du 8 juillet 2015 comme « *une première évaluation par écrit, d'une autorité compétente, qu'elle soit administrative ou judiciaire, concluant, sur la base de faits concrets, à l'existence d'une irrégularité, sans préjudice de la possibilité que cette conclusion soit à réviser ou à retirer ultérieurement à la suite des développements de la procédure administrative ou judiciaire* ».

Le « soupçon de fraude » est défini dans le même règlement délégué n° 2015-1970 comme « *une irrégularité donnant lieu à l'engagement d'une procédure administrative ou judiciaire au niveau national afin de déterminer l'existence d'un* comportement *intentionnel (…) lequel apparaît suite à l'analyse de l'irrégularité (faux documents, répétition volontaire de l'erreur, fausse déclaration…)* ».

L'Office européen de lutte antifraude (OLAF) est chargé du recueil et du traitement des cas signalés pour le compte de la Commission européenne.

[133] Voir l'article 125-4 c) du règlement n° 1303-2013 du 17 décembre 2013

[134] Y compris dans le cas où aucun paiement n'a été préalablement effectué en faveur du bénéficiaire au titre de la part UE et/ou nationale (Voir article 3-n du règlement délégué n° 2015-1970 du 8 juillet 2015)

Les programmes de la période 2021-2027

Le Règlement (UE) 2021/1060 du Parlement européen et du Conseil du 24 juin 2021 porte les dispositions communes pour la mise en œuvre des programmes de la politique européenne de cohésion pour la génération 2021-2027.

Selon le schéma en usage, ce règlement distingue :

- Les prérogatives et responsabilités des Etats membres (article 69) ;
- Les prérogatives et responsabilités de la Commission (article 70) ;
- Les prérogatives et responsabilités des autorités de gestion en charge de l'exécution des programmes (articles 72 à 74) ;
- Les prérogatives et responsabilités de l'autorité d'audit (articles 77 à 82).

Par ailleurs, l'article 76 crée une fonction comptable en charge de l'établissement et de la vérification des demandes de paiement présentées à la Commission au fil de l'exécution des programmes ; cette fonction peut être intégrée à l'autorité de gestion ou être confiée à un organisme tiers.

Du fait de leur caractère de nouveauté et dans l'attente de la publication de futurs règlements délégués, il n'est pas utile de présenter ces dispositions dans leur détail.

Il convient cependant de signaler un important changement apporté par l'article 74-2 qui invite les autorités de gestion à réaliser les vérifications de premier niveau, avant mise en paiement de l'aide communautaire due, sur la base d'une analyse préalable des risques ; cette mesure vise à adopter une approche proportionnée des contrôles propre à réduire la charge administrative supportée par le bénéficiaire final sans compromettre l'assurance donnée sur la qualité de gestion.

En conséquence, les autorités de gestion en charge des programmes de la période 2021-2027 seront amenées à apporter une attention croissante à la mise en place ainsi qu'à l'actualisation de la cartographie des risques liés à l'utilisation des financements européens.

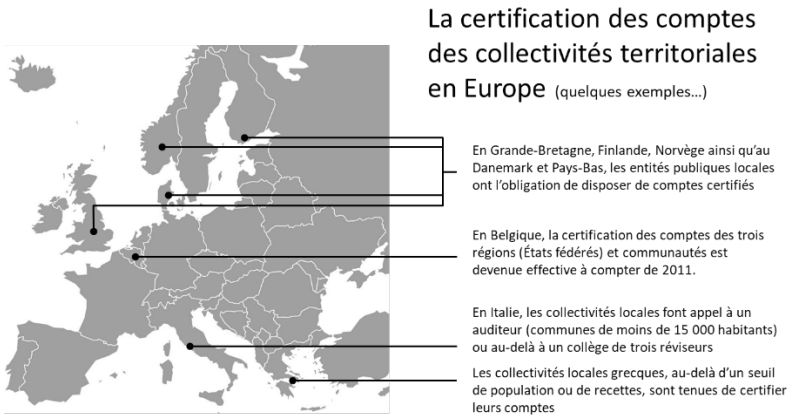
Cette attention soutenue devra notamment se traduire en termes de méthodologie employée et de suites opérationnelles données.

Fiche technique 4

Expérimentation de la certification des comptes dans les collectivités locales (2017-2023)

La certification des comptes se définit comme la délivrance, chaque année, par un auditeur externe, indépendant et respectant les normes professionnelles communément admises, d'une opinion attestant que les comptes soumis à l'autorité gestionnaire sont réguliers, sincères et donnent une image fidèle du patrimoine, de la situation financière et du résultat des opérations de l'exercice.

L'exercice est couramment pratiqué dans les collectivités territoriales de l'espace européen.



En France, la certification des comptes du secteur public a d'abord été instituée pour l'Etat, la plupart des établissements publics, les organismes nationaux, les hôpitaux et les universités, sans toucher les collectivités territoriales.

Toutefois, une tendance de fond se dessine pour la généralisation de cette pratique.

En premier lieu l'article 47-2 de la loi constitutionnelle n° 2008-724 du 23 juillet 2008 de modernisation des institutions de la Ve République dans son article 47-2 a réaffirmé le principe selon lequel « *les comptes des administrations publiques sont réguliers et sincères (et) donnent une image fidèle du résultat de leur gestion, de leur patrimoine et de leur situation financière*. »

De même, la directive 2011/85/UE du 8 novembre 2011 sur les exigences applicables aux cadres budgétaires des Etats membres prévoit que les « *systèmes de comptabilité publique [des Etats membres] sont soumis à un contrôle interne et à un audit indépendant* » (article 3-1).

En réponse, les autorités nationales ont fait le choix d'une expérimentation couvrant un échantillon représentatif des collectivités existantes en vue de définir les modalités les mieux appropriées à une généralisation ultérieure.

L'article 110 de la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République (loi NOTRe) a ainsi permis aux collectivités et à leurs groupements de se porter candidates à une expérimentation permettant d'établir les conditions préalables et nécessaires à la mise en place de la certification du secteur public local.

A la fin de l'année 2016, vingt-cinq collectivités expérimentatrices ont été désignées : deux Régions, six Départements, dix Communes, six Etablissements publics de coopération intercommunale et un Syndicat [135].

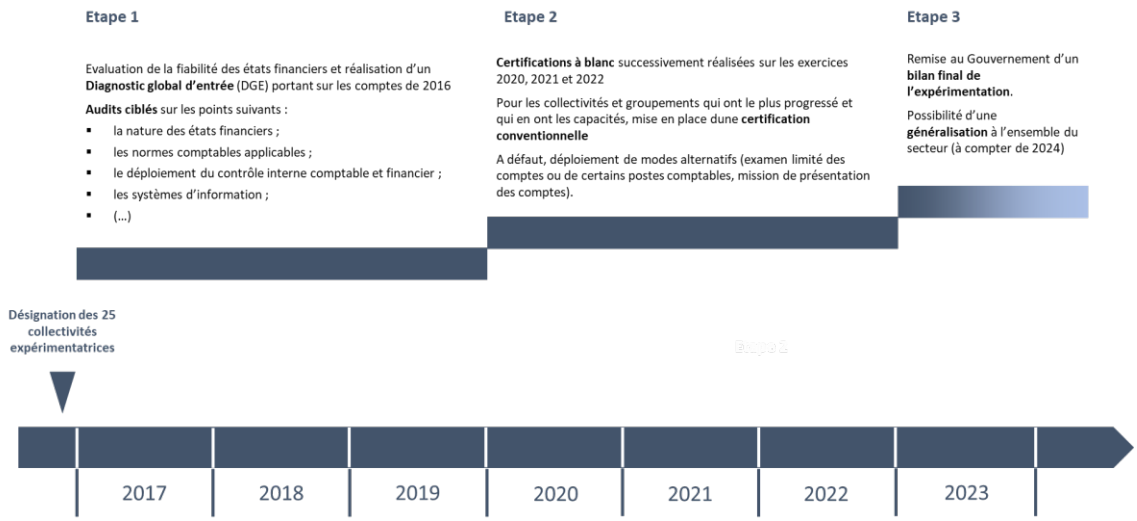
Toutes sont appelées à remplir le même cahier des charges ; pour ce faire elles disposent d'un accompagnement méthodologique et technique des Chambres régionales des comptes, sous la supervision globale de la Cour des comptes.

Un cahier des charges de l'expérimentation a été proposé aux Commissaires aux comptes désignés par les collectivités expérimentatrices [136]; celles-ci ont été accompagné par des formations inter-juridictionnelles (FIJ), composés de magistrats des Chambres régionales des comptes, de la Cour des Comptes, et d'experts désignés (commissaires aux comptes, experts certification.

L'expérimentation / La démarche expérimentale dans son ensemble s'étend sur une période de sept années répartie en trois phase :

- Une phase de préparation couvrant les années 2017-2019 vise à une évaluation de la fiabilité des états financiers et à la réalisation d'un Diagnostic global d'entrée portant sur les comptes de 2016. A l'issue du Diagnostic global d'entrée, des audits ciblés ont été menés sur diverses thématiques en résonance avec les enjeux associés à la Certification des comptes.
- Une phase de test couvrant les années 2020-2023 est consacrée à la réalisation de certifications conventionnelles sur les exercices 2020, 2021 et 2022 et à la recherche des méthodes les mieux adaptées à chaque contexte.
- Une phase de bilan en 2023 a pour objet de consolider les enseignements tirés des expérimentations menées et d'en tirer des propositions pour une généralisation éventuelle du dispositif, à compter de l'année 2024.

<u>Calendrier de l'expérimentation de la certification des comptes</u>



[135] Voir l'arrêté du 10 novembre 2016 fixant la liste des collectivités territoriales et groupements admis à intégrer le dispositif d'expérimentation de la certification de leurs comptes (JORF n°0267 du 17 novembre 2016 -texte n° 41)

[136] Ce cahier des charges a été élaboré par la Cour des comptes, en tant que pilote global de l'expérimentation (selon les termes de la loi NOTRe). La Cour des comptes exerce également un contrôle de conformité des prestations des Commissaires aux comptes.

A terme, la certification des comptes locaux devrait s'articuler avec l'achèvement du recueil des normes comptables[137] et l'examen des dérogations existantes aux principes comptables généraux.

Vue synthétique des différentes expérimentations menées au cours de la période 2020 - 2023[138]

Dispositif / Catégories de collectivités	Régions	Départements	Communes	EPCI
Le cadre de présentation des comptes				
Compte financier unique	Expérimentation à compter des comptes de l'exercice 2020, en application des dispositions de l'article 242 de la Loi de finance initiale pour 2019 (deux vagues proposées ; recensement des candidatures jusqu'au 27 juin 2019)[139]			
Certification des comptes et « dispositifs alternatifs »				
Certification légale des comptes	Expérimentation auprès de 25 collectivités locales menée depuis 2017 (article 110 de la loi NOTRe) et pilotée par la Cour des comptes			
Examen limité des comptes et mission d'attestation particulière			Propositions de la Cour des comptes à l'attention de certaines collectivités appartenant au périmètre des 25 collectivités locales (article 110 de la loi NOTRe)	
Attestation de fiabilité des comptes	Lancement de l'expérimentation en 2019 sur la base d'un recensement des candidatures initié par la DGFiP auprès de collectivités ne relevant pas du périmètre des 25 collectivités locales (article 110 de la loi NOTRe)			
Synthèse sur la qualité des comptes présentée à l'assemblée délibérante			Lancement de l'expérimentation en 2020 sur la base d'un recensement des candidatures initié par la DGFiP	

Le processus en cours s'inscrit ainsi dans la mise en place programmée d'un référentiel budgétaire et comptable unique associant compte administratif et compte de gestion qui serait garant d'une meilleure collaboration entre ordonnateurs et comptables, mais aussi renforcerait la lisibilité des actions menées auprès de l'ensemble des parties engagées (assemblées délibérantes, usagers et citoyens).

[137] Le Conseil de normalisation des comptes publics (CNOCP) est étroitement associé à ces travaux - cf. notamment le référentiel M 57 applicable aux collectivités territoriales uniques, aux métropoles et à leurs établissements publics administratifs

[138] Source DGFiP_Bureau CL1B « Comptabilités locales »

[139] Trois nouvelles vagues de collectivités sont retenues pour la période 2021-2023, soit un total de 2500 collectivités environ engagées dans cette démarche. Le gouvernement rendra un rapport au Parlement sur l'expérimentation au plus tard le 15 novembre 2023 : https://www.collectivites-locales.gouv.fr/files/Finances%20locales/8.%20avoir%20des%20comptes%20bien%20tenus/2021/CFU/Guide_CFU_v1.3_12nov2021.pdf

Bilan à mi-parcours

En juin 2019, la Cour des Comptes a publié un « Bilan intermédiaire de l'expérimentation de la certification des comptes locaux »

Ce bilan repose sur les résultats des Diagnostics globaux d'entrée réalisés en 2017 et 2018 dans les 25 collectivités expérimentatrices.

Il en ressort que la plupart d'entre elles n'ont pas réuni les conditions nécessaires pour disposer d'une information suffisante sur leurs processus comptables et financiers ainsi que les dispositifs de maîtrise des risques encourus au titre de leurs diverses activités.

En premier lieu, les dispositifs de maîtrise des risques comptables et financiers sont généralement pointés comme insuffisants, en particulier pour ce qui concerne l'actif immobilisé, les créances et stocks et les engagements hors bilan.

De nombreux facteurs concourent à cette situation :

- les immobilisations, les achats, les charges de personnel ou les dépenses sociales sont rarement suivis de manière formalisée et documentée ;
- des biais de périmètre affectent souvent l'appréciation et le suivi des risques auxquels les collectivités sont soumises, les budgets annexes sont ainsi fréquemment exclus de la démarche ;
- les compétences transférées ne donnent pas toujours lieu à la comptabilisation des actifs correspondants ;
- la fréquence trop faible des mises à jour des données financières, comme les actifs de la collectivité (intégrant amortissements et dépréciations) peut entraîner des écarts significatifs entre l'inventaire de l'ordonnateur et l'état d'actif du comptable public ; certaines collectivités se trouvent ainsi dans l'impossibilité de déterminer avec précision la valeur de ces actifs ;
- les relations avec les satellites des collectivités sont, de manière générale, insuffisamment recensées et connues (niveaux de participations financières, dépréciation des titres, recapitalisation, garanties d'emprunts…) ; les engagements hors bilan des collectivités découlant notamment des conventions signées avec les tiers sont souvent mal documentés ;
- enfin, peu de collectivités mettent en place des provisions pour dépréciation de créances ou pour risques et charges (risque de contentieux, risque en cas de procédure…).

En deuxième lieu, le défaut d'urbanisation des systèmes d'information financière est un obstacle couramment relevé à la certification des comptes, notamment sur la question de l'articulation entre le « cœur comptable » et les applications « métier ».

Le traitement des informations comptables et financières est fragilisé par la faible interopérabilité des applications engagées dans l'engagement et le suivi des dépenses ; ainsi que cela a pu être observé dans la plupart des collectivités.

Plus généralement, la Cour relève que beaucoup reste à faire pour assurer la maîtrise les risques informatiques, y compris en matière de contrôles généraux (gestion des droits et de sécurité des accès aux systèmes d'information, …)

En troisième lieu, la plupart des diagnostics ont montré la nécessité de développer un dispositif de contrôle interne comptable et financier parfaitement robuste et complet.

La Cour a pu constater que le contrôle des risques comptables et financiers est dans la plupart des cas insuffisant et peu transparent pour un auditeur.

Elle attend donc que soit mise en œuvre une démarche de contrôle interne impliquant une répartition des tâches claire et cohérente adossée à une documentation suffisante, tout en proportionnant ces exigences au degré de maturité des collectivités expérimentatrices.

Une dernière observation concerne l'absence presque toujours vérifiée de services chargés de manière transversale de l'audit interne et indépendants des services assurant le contrôle interne ; cette situation fragilise le dispositif assurantiel des collectivités concernées.

Récapitulatif des principaux constats des Diagnostics globaux d'entrée[140]

Difficultés pour obtenir une image fidèle et sincère de la situation financière

- Absence de tenue de l'inventaire comptable de l'actif immobilisé
- Absence fréquente de comptabilité de stocks
- Provisions insuffisantes au regard des engagements
- Recensement des engagements hors bilan à améliorer
- Insuffisance récurrente des rattachements de charges et de produits à l'exercice

Périmètre des entités et des incidences financières insuffisamment déterminé

- Transcription imparfaite dans les états financiers des changements de champs de compétences géographiques et/ou fonctionnels
- Recensement souvent lacunaire des satellites des collectivités

Recensement et contrôle insuffisants des systèmes d'information

- Carte des systèmes d'information souvent incomplète

Amélioration nécessaire du dispositif de maîtrise des risques comptables et financiers

- Absence de dispositifs formalisés de contrôle interne
- Absence d'une fonction transversale de maîtrise des risques
- Absence d'assurance raisonnable sur la fiabilité des informations comptables financières

[140] Tels que présentés dans le « Bilan intermédiaire de l'expérimentation de la certification des comptes locaux » publié par la Cour des Comptes en juin 2019 - Il n'est aucunement question ici d'évoquer la situation particulière de telle ou telle autre collectivité expérimentatrice

Poursuite de l'expérimentation - Perspectives de la phase de test (2020-2023)

En réponse aux Diagnostics globaux d'entrée, les collectivités expérimentatrices ont été invitées à mener à bien des plans d'action comprenant les différentes mesures correctrices requises.

Pour celles qui ont le plus progressé - et qui en ont les capacités techniques et les moyens - une certification conventionnelle sera assurée par un commissaire aux comptes sélectionné à cet effet, suivant un cahier des charges préalablement défini par la Cour des comptes.

Cette certification couvre la nature des états financiers, la correcte application des normes comptables pertinentes, le déploiement effectif du contrôle interne comptable et financier ainsi que le bon fonctionnement des systèmes d'information utilisés.

Le cas échéant, il pourra être proposé aux collectivités n'atteignant pas les standards requis de tester d'autres modes d'appréciation de la fiabilité de leurs comptes.

Au regard des constats réalisée à l'issue de la première phase et en tenant compte de leurs capacités techniques et humaines, ces modes alternatifs pourront prendre la forme d'un examen limité des comptes ou de certains postes comptables, ou encore d'une mission de présentation des comptes ; la réalisation de ces travaux devrait échoir à des professionnels du chiffre (experts-comptables, commissaires aux comptes) et éventuellement à la Direction générale des finances publiques.

Pour aller plus loin…

Le « Bilan intermédiaire de l'expérimentation de la certification des comptes locaux » publié par la Cour des Comptes en juin 2019 est la source d'information la plus directe et la plus complète sur l'état d'avancement des travaux engagés et les perspectives attendues.

Par ailleurs, différentes lectures combinées peuvent donner une bonne idée d'ensemble des enjeux, du mode opératoire et des conditions de succès attendues.

<u>Publications</u>

- Qualité et certification des comptes des collectivités territoriales - Enjeux et outils de fiabilisation Territorial Editions - Juin 2018

<u>Articles</u>

- La certification des comptes des collectivités : une démarche de modernisation de la gestion publique locale - Les Cahiers de la fonction publique - Avril 2016
- La certification des comptes des collectivités, outils de qualité comptable et de transparence - La Semaine juridique - Edition administrations et collectivités territoriales - 13 mars 2017
- Certification des comptes : attention aux bouleversements systémiques - La lettre du cadre territorial - Mai 2018
- Finances locales - Fiabilités des comptes : chantiers en cours - La Gazette des Communes - 26 novembre 2018

Enfin, des pistes intéressantes pour la mise à niveau des dispositifs de contrôle interne peuvent être trouvées dans le « Guide de renforcement du contrôle interne comptable et financier dans les collectivités locales » édité par la Délégation générale des finances publiques (DFGIP) en mai 2019.

Fiche technique 5

Mode opératoire pour la mise en place d'un système de management de la continuité d'activité

Le mode opératoire pour la mise en place d'un système de management de la continuité d'activité prend appui sur la Norme ISO 22301-2019 relative à la Sécurité et à la résilience des organisations confrontées à des risques majeurs[141].

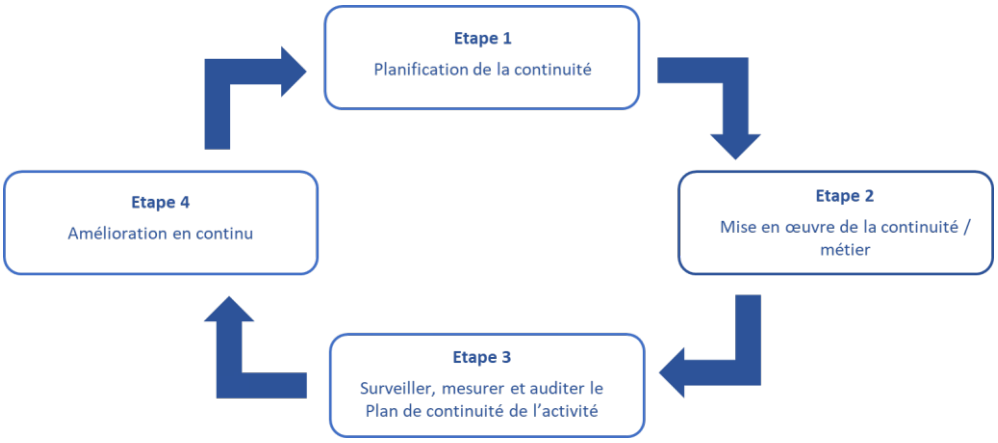
Il se décline en quatre étapes successives :

- planification de la continuité ;
- mise en œuvre de la continuité ;
- vérification de la robustesse et de l'efficience du dispositif créé (tests, contrôle, audit) ;
- amélioration en continu au regard des enseignements tirés de l'expérience réelle et/ou des vérifications opérées.

Les opérations réalisées à chaque étape alimentent un mécanisme assurantiel garant de la pérennité du fonctionnement de l'organisation et de la qualité du service rendu.

Dans les développements qui suivent, le terme « organisation » est utilisé pour désigner la collectivité.

Processus de mise en place et d'amélioration *in itinere* du Système de management de la continuité d'activité



[141] Ce référentiel prend appui et prolonge la Norme BS 25999 *Business continuity planning* publiée par l'organisme British Standards Institute en apportant plus de détails sur la fixation des objectifs de l'organisation, le suivi de la performance et des indicateurs.

Au préalable, l'organisation doit déterminer et mettre à disposition les ressources nécessaires pour établir, mettre en œuvre et maintenir le Système de management de la continuité d'activité.

L'organisation des acteurs du Plan de continuité d'activité et leurs rôles respectifs doivent être précisément définis.

La Direction générale de l'organisation doit désigner un responsable en charge de la politique Plan de continuité d'activité et de sa diffusion.

A toutes les étapes qui suivent, la documentation relative au Plan de continuité d'activité doit être lisible, aisément identifiable et traçable.

L'organisation s'assure qu'elle est stockée, protégée et disponible sans délai.

Elle réalise des contrôles réguliers afin de s'assurer que :

- les documents ont été approuvés et validés ;
- les documents ont été révisés, mis à jour et revalidés ;
- les mises à jour et modifications apportées sont identifiables ;
- les documents d'origine externe sont identifiés et leur diffusion contrôlée ;
- les documents devenus obsolètes sont retirés ou clairement identifiés par rapport aux documents maintenus.

Première étape - Planifier la continuité

L'organisation doit identifier ses activités critiques et apprécier les ressources minimales nécessaires pour fonctionner en mode dégradé.

Il lui revient ensuite de reconnaître les menaces qui pèsent sur ces activités et déterminer des actions appropriées pour minimiser les risques identifiés.

a) Identification des activités critiques

L'identification des activités critiques doit permettre :

- d'obtenir une compréhension des services clés de l'organisation ainsi que des processus dont ils dépendent ;
- de déterminer les activités prioritaires pour l'organisation et leur délai maximum d'interruption ;
- d'identifier les ressources clés nécessaires à la continuité et à la relève des activités ;
- de mesurer les dépendances internes et externes.

A cet effet, l'organisation réalise une étude d'impact sur les activités comprenant :

- l'identification des activités et processus critiques au sein de l'organisation, dépendant de fournisseurs ou de toute autre partie prenante ;
- l'analyse des impacts qui résulteraient d'un arrêt des activités et processus critiques, en graduant cet impact selon la durée de l'arrêt.

L'étude d'impact sur les activités inclut également :

- la détermination du temps d'arrêt ou d'indisponibilité maximum admissible des processus et activités critiques,
- une estimation des ressources humaines et matérielles nécessaires à la reprise de chaque activité critique.

b) Mise en place d'une cartographie des risques

L'analyse des risques doit permettre à l'organisation de comprendre les menaces et vulnérabilités qui pèsent sur ses activités critiques et celles de ses partenaires, fournisseurs et autres parties prenantes.

Le but de l'évaluation des risques est de fournir des informations factuelles et des analyses pour prendre des décisions éclairées sur la façon de traiter les risques.

Ce travail permet à l'organisation de comprendre les impacts qu'engendrait une crise sur ses activités.

Pour chacune des activités critiques, l'organisation identifie des mesures permettant :

- de réduire la probabilité d'occurrence d'un arrêt des activités et dans tous les cas de contenir au minimum tout risque d'interruption brutale ;
- de limiter les impacts d'un arrêt sur les activités.

Deuxième étape - Mettre en œuvre de la continuité

Cette seconde étape comprend elle-même deux phases.

a) Mise en place d'une stratégie de continuité globale d'activité

Il s'agira pour l'organisation de prendre les dispositions nécessaires pour gérer la situation de crise et reprendre ses activités cruciales dans le délai cible de rétablissement qui aura été estimé admissible.

La stratégie de continuité d'activités constitue la base pour les plans de continuité d'activités.

Cela nécessite de la part de l'organisation de :

- fixer un mode opératoire pour la des activités cruciales dans le délai cible de rétablissement défini au préalable en incluant les ressources nécessaires ;
- déterminer les ajustements à apporter à ses liens contractuels et partenariaux avec les fournisseurs et toute autre partie nécessaire à son action.

Une fois les processus critiques identifiés ainsi que leurs ressources associées, il s'agit de déterminer une stratégie globale (site de repli et postes de travail, reprise de l'informatique…)

Une stratégie détaillée doit également être définie : reprise par activité, fonctionnement des processus en mode dégradé.

b) Elaboration d'un Plan de continuité d'activité

L'organisation doit établir des procédures documentées lui permettant de répondre à un incident perturbateur et de poursuivre ou rétablir ses activités dans un délai prédéterminé.

A cet effet elle établit un Plan de continuité d'activité

Dans tous les cas et *a minima* un Plan de continuité d'activité doit définir :

- le but et le domaine d'application ;
- les objectifs poursuivis ;
- la présentation des activités critiques de l'organisation ;
- les procédures dégradées ;
- les rôles et responsabilités du projet ;
- les interdépendances et interactions internes et externes ;
- les exigences en termes de ressources ;
- les processus relatifs au flux d'informations et à la documentation ;
- la composition de la cellule de crise ;
- le schéma d'alerte ;
- les annuaires de crise.

Les composantes et le contenu du Plan de continuité d'activité varient selon les contextes.

Il peut ainsi être intéressant de le scinder en plusieurs « PCA métier » ou encore constituer un Plan de gestion de crise distinct, ces éléments étant à l'appréciation de l'organisation.

Le Plan de continuité d'activité est actualisé en continu, selon le processus décrit aux deux étapes suivantes.

Troisième étape - Surveiller, mesurer et auditer le Plan de continuité de l'activité

L'organisation est tenue d'éprouver de manière régulière la robustesse du Plan de continuité de l'activité et de mesurer son efficience au regard des moyens déployés et des objectifs poursuivis.

A cet effet, il lui appartient de définir dans un plan spécifique ce qu'il convient de mesurer, surveiller et évaluer.

Le plan ainsi élaboré prend appui sur les trois éléments suivants.

a) Exercices et tests réguliers

L'organisation s'assure que le plan de continuité d'activités mis en œuvre a été validé par des tests et exercices puis ajusté en fonction des résultats obtenus.

Ces exercices doivent permettre de vérifier l'adéquation du Plan de continuité de l'activité avec les exigences liées à l'activité.

b) Retour sur expérience de tout événement ayant déclenché l'activation du Plan de continuité de l'activité

Tout évènement ayant entraîné le déclenchement du Plan de continuité d'activité doit donner lieu à un processus de révision intégrant les points suivants :

- spécification de la nature et de la cause de l'évènement ;
- évaluation de la qualité de réponse de l'organisation à cet évènement ;
- mesure de l'efficacité de l'organisation par rapport au délai-cible de rétablissement ;
- identification des améliorations éventuelles à apporter.

c) Audit interne

L'organisation doit s'assurer que les audits du système sont prévus et réalisés à intervalles réguliers afin de déterminer si le Système de Management de la Continuité d'Activité :

- est conforme aux dispositions du Plan de continuité de l'activité ;
- a été correctement mis en place et suivi ;
- fait le lien entre la politique du Plan de continuité d'activité et les objectifs de l'organisation, tels que traduits dans le projet de mandat et le projet d'administration.

Le programme d'audit doit être planifié, mis en œuvre et suivi en prenant appui sur l'identification des activités critiques, l'évaluation des risques, les mesures de réduction de ces risques ainsi que sur le résultat des audits précédents, le cas échéant.

Quatrième étape - Améliorer en continu

L'organisation est tenue de réviser en continu son plan de continuité d'activités afin de s'assurer de son adéquation et de son efficience.

Ces révisions devront être planifiées mais également effectuée lors de changements significatifs dans l'organisation.

Les points pris en compte dans le processus de révision sont :

- les niveaux des risques résiduels et d'acceptation de ces risques ;
- les résultats des exercices et tests réalisés pour mesurer le degré de vulnérabilité de l'organisation ;
- les retours d'expérience de tout incident survenu ;
- le degré d'avancement des actions préventives et correctrices visant à la maîtrise des risques majeurs identifiés ;
- les résultats des audits du Système de management de la continuité d'activité de l'organisation ainsi que ceux de ses partenaires stratégiques, le cas échéant ;
- les propositions de suivi de bonnes pratiques notamment dans le cadre de travaux de benchmarking.

Fiche technique 6

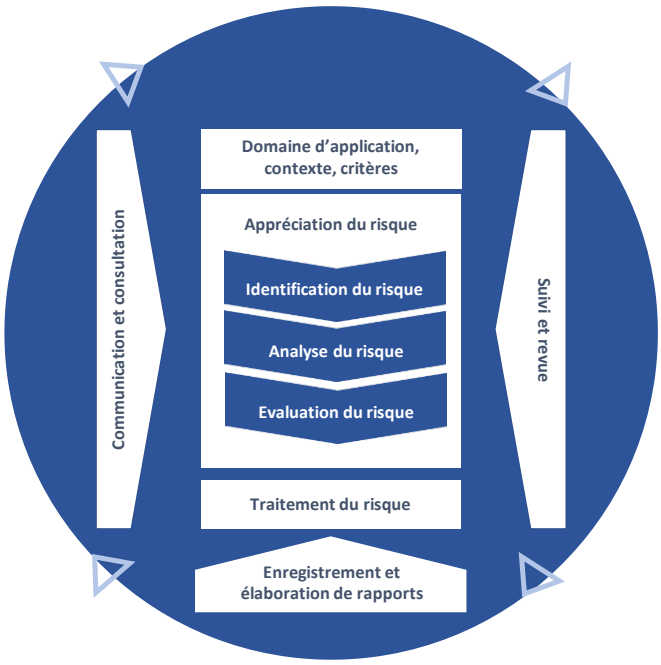
Le processus de management du risque

La norme ISO 31000-2018 relative au management du risque comprend une définition du processus méthodologique permettant au dispositif d'être structuré, de bénéficier d'une méthodologie d'analyse des risques claire et homogène au sein de la collectivité.

L'application de ce processus doit être systématique et partagé.

Son appropriation et sa déclinaison opérationnelle constituent deux enjeux importants.

Processus de management du risque



Source : Norme ISO 31000-2018 « Management du risque » (Fig 4)

Référence [142]	Etapes du processus	Commentaires
Article 6.2	Communication et concertation	Témoignant de la place, du rôle et des attendus des parties prenantes dans le dispositif de management du risque, la communication permettant une sensibilisation et une compréhension du risque, et la concertation, l'échange et l'expression d'un avis ; elles « *expriment la dimension collaborative et inclusive voulue par la norme pour le dispositif de management du risque* »[143] ;
Article 6.3.2	Définition d'un domaine d'application	Comme pour tout processus, des objectifs doivent être fixés, en déterminant également son périmètre - qui peut être limité à une entité, une activité, un risque - étant entendu qu'une approche systémique confortera la richesse d'un tel dispositif.
Article 6.3.3	Etablissement du contexte	La bonne fin de la démarche est conditionnée à la prise en compte et l'analyse d'éléments de contexte interne et externe.
Article 6.3.4	Définition des critères de risque	Ces critères permettent à la collectivité de se positionner sur le niveau et le type de risque pouvant être pris ou non, en fonction des objectifs. Ces critères aideront à s'assurer que les risques pris sont effectivement souhaités et correspondent à une stratégie assumée. Ayant un caractère dynamique, ils peuvent être actualisés en fonction des évolutions du contexte.
Article 6.4	Appréciation du risque	Menée de façon itérative, systématique et collaborative, cetté étape comprend trois phases distinctes : identification, analyse et évaluation du risque.
Article 6.5	Traitement du risque	Sur la base d'un rapport coût-avantage et en tenant compte de l'appétence au risque de la collectivité, des dispositions sont proposées pour traiter le risque : suppression (via le retrait de l'activité concernée), maintien, transfert/mutualisation, mise en œuvre des mesures de maîtrise appropriées.
Article 6.6	Suivi et revue	Cette étape est nécessaire pour s'assurer du bon fonctionnement du processus et améliorer son efficacité. Le suivi porte sur les différents volets du processus et concernant tant sa conception, que sa mise en œuvre et ses résultats obtenus.
Article 6.7	Enregistrement et élaboration de rapports	Le processus et les résultats obtenus doivent être documentés afin de disposer d'une traçabilité des actions. Cet exercice contribue par ailleurs à l'appropriation méthodologique et à la démonstration des réalisations effective, ses modalités d'élaboration sont déterminées par la gouvernance.

[142] Norme ISO 31000

[143] Management du risque : une approche stratégique ; Géraldine SUTRA ; Afnor éditions ; 2018 ; 188 pages

Fiche technique 7

Les trois lignes de maîtrise des risques

La demande de différenciation des différents niveaux de contrôle, de leurs rôles et de leurs responsabilités propres résulte de l'extension du champ couvert par le management des risques dont l'entrée en vigueur du COSO 2013 a marqué un jalon déterminant ; tous les domaines de l'organisation sont désormais concernés, du risque stratégique à ceux liés aux domaines opérationnels, financiers et de conformité.

Un tel périmètre concerne nécessairement l'ensemble des activités de l'organisation.

Aussi il est apparu pertinent de répartir ces activités entre trois groupes de fonctions diversement impliquées dans la gestion des risques :

- les fonctions qui endossent et gèrent les risques ;
- les fonctions qui assurent le suivi des risques ;
- les fonctions qui fournissent une assurance indépendante.

A ces trois groupes s'ajoute l'action des auditeurs externes ou des autorités de régulation en charge de certifier le fonctionnement de l'organisation au regard des normes applicables.

Première ligne de maîtrise - Les managers propriétaires des risques

La première ligne de maîtrise des activités est constituée par les managers opérationnels, responsables de l'évaluation et de la diminution des risques, notamment au travers d'un dispositif de contrôle adéquat, portant sur les processus dont ils ont la charge.

Cette première ligne permet la maîtrise des activités au quotidien en mettant en œuvre les pratiques les plus efficaces de gestion des risques au niveau de chaque processus et en communiquant les informations appropriées à la deuxième ligne de maîtrise.

Les managers sont dits « propriétaires » des risques associés aux domaines dont ils ont la charge. A ce titre, ils pilotent l'élaboration et la mise en œuvre des règles et procédures internes et s'assurent que les activités sont compatibles avec les objectifs fixés. Ils ont également la responsabilité de la mise en œuvre des mesures correctives permettant de remédier aux déficiences des processus et des contrôles.

Dans le cadre d'un système de responsabilité en cascade, le management intermédiaire définit et met en place des procédures de contrôle détaillées puis en supervise l'application à chaque échelon de la chaîne de traitement.

Des contrôles managériaux et de supervision adéquats assurent la conformité et le cas échéant mettent en évidence des contrôles défaillants, des processus inadéquats ou des événements inattendus.

Seconde ligne de maîtrise - Les fonctions de gestion des risques, de conformité et de reporting

La deuxième ligne de maîtrise est constituée des services fonctionnels responsables de domaines d'expertise et des fonctions dédiées à l'animation du dispositif global de maîtrise des risques.

Ces services disposent d'une expertise et d'un savoir-faire uniques pour l'analyse des organisations et de compétences essentielles en matière d'activités de contrôle.

Ils sont chargés de la structuration et de la surveillance des contrôles relevant de la première ligne de maîtrise et apportent un soutien aux opérationnels pour la conception et le déploiement des contrôles les plus pertinents.

Plus largement ils fournissent aux managers un appui dans l'identification et l'évaluation des principaux risques relevant de leur domaine d'activité.

Ces différents travaux s'inscrivent dans trois fonctions distinctes :

- une fonction de gestion des risques qui facilite et surveille la mise en œuvre de dispositifs efficaces de gestion des risques par le management et qui assiste les propriétaires des risques dans la définition du niveau cible d'exposition aux risques et la communication d'informations adéquates en matière de risques dans l'ensemble de l'organisation ;
- une fonction de conformité chargée de surveiller divers risques spécifiques tels que le non-respect des lois et réglementations en vigueur ;
- une fonction de contrôle de gestion qui effectue le suivi des risques financiers et du reporting financier.

Ces fonctions sont indépendantes de la première ligne de maîtrise et s'analysent comme des fonctions support du management.

La seconde ligne de maîtrise joue ainsi un rôle essentiel dans la conception, la sécurisation et le pilotage du système de management des risques.

Cependant, et du fait précisément de son implication dans ce processus, elle n'a pas la capacité de produire des analyses indépendantes concernant les dispositifs de gestion des risques et de contrôle interne.

Troisième ligne de maîtrise - L'audit interne

En tant que troisième ligne de maîtrise des activités, une fonction d'audit interne fournit, à travers une approche fondée sur le risque, une assurance globale aux instances de surveillance et à la direction générale de l'organisation.

Cette assurance globale couvre l'efficacité des deux premières lignes de maîtrise et de la gouvernance de l'organisation.

L'assurance donnée par l'audit interne couvre :

- un large éventail d'objectifs, liés notamment à l'efficience et à l'efficacité des opérations, à la protection de biens mobiliers et immobiliers, à la fiabilité et à l'intégrité des processus de reporting et à la conformité aux lois, règlementations, normes, procédures et contrats ;
- toutes les composantes du référentiel de gestion des risques et de contrôle interne, qui incluent l'environnement de contrôle, l'identification des risques, leur évaluation et leur traitement, l'information et la communication, ainsi que le pilotage ;
- l'ensemble de l'entité, des divisions, unités opérationnelles et fonctions support.

L'audit interne contribue ainsi activement à l'efficacité du dispositif de gouvernance d'une organisation sous réserve que les conditions suivantes soient remplies :

- appliquer les normes nationales et internationales généralement admises pour la pratique de l'audit interne ;
- être rattaché à un niveau suffisamment élevé dans l'organisation pour pouvoir assurer ses responsabilités de manière indépendante ;
- avoir une relation étroite et effective avec le Conseil ou l'organe de gouvernance équivalent.

Auditeurs externes, régulateurs et autres organes externes

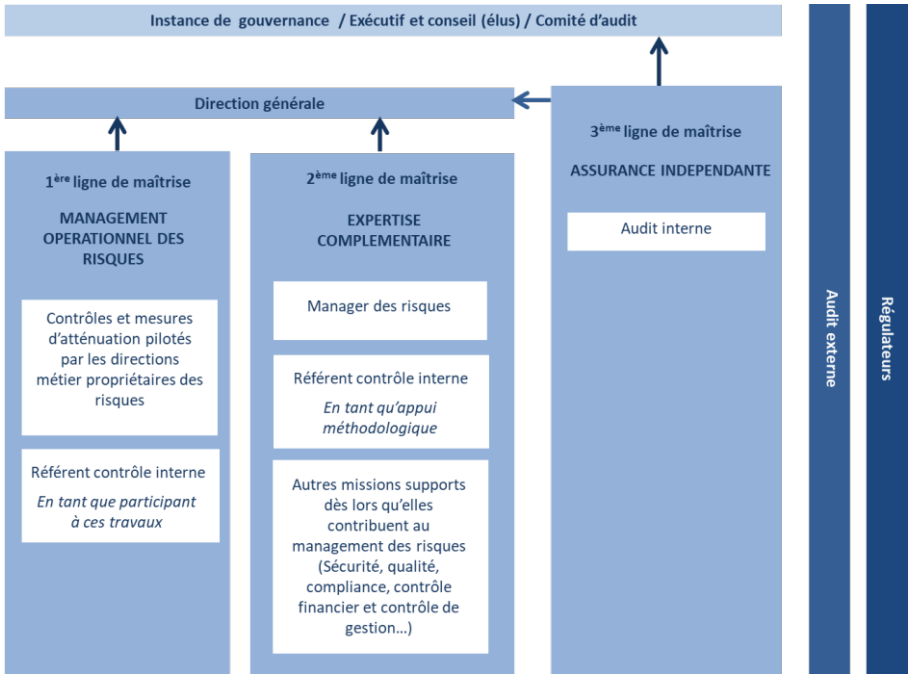
Des auditeurs externes, les régulateurs et d'autres instances habilitées sont amenés à intervenir dans le dispositif global de gouvernance et de contrôle d'une organisation. Leur rôle est variable selon le secteur d'activité concerné et la réglementation qui y est applicable.

Il arrive que ces organismes extérieurs expriment des exigences visant à renforcer les contrôles au sein des organisations et procèdent ponctuellement à des revues indépendantes et objectives afin d'évaluer en tout ou partie les première, deuxième ou troisième ligne de maîtrise à l'aune de ces exigences.

Sous réserve d'une coordination efficace, les auditeurs externes, les régulateurs et d'autres groupes externes peuvent être considérés comme des lignes de maîtrise supplémentaires, qui fournissent une assurance aux parties prenantes de l'organisation, notamment à ses organes de gouvernance. Leur intervention est garante du bon fonctionnement du système de management des risques d'une organisation.

Les préconisations et recommandations qu'ils sont amenés à formuler peuvent également concourir à son amélioration et/ou à la correction d'éventuels dysfonctionnements.

Le schéma suivant[144] peut être utilisé pour représenter les trois lignes de maîtrise des risques.



[144] Ce schéma a été fixé dans le cadre des lignes directrices de l'ECIIA (European Confederation of Institutes of Internal Auditing) et de la FERMA (Federation of european risk management associations) sur la huitième directive de l'UE relative au droit des sociétés

Fiche technique 8

Profils engagés dans une démarche de management et de maîtrise des risques - Acteurs en charge de la gouvernance

La gouvernance se partage entre la Direction générale et l'Exécutif ; elle peut s'aider d'une instance de suivi et de pilotage tel qu'un comité des risques et/ou un comité d'audit.

Les missions qui lui sont imparties peuvent se résumer dans les Principes n°1 à 5 du cadre de référence du COSO-ERM qui définit les dispositifs de management des risques dans toute organisation privée ou publique.

L'importance donnée à la gouvernance se retrouve également dans Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP) qui lui dédie en particulier la Norme 2110.

De manière significative, le CRIPP prévoit que le responsable de l'audit interne apporte une assurance et des conseils à la direction générale et au Conseil en ce qui concerne les processus de gouvernance (Norme 2110) avant même d'aborder le management des risques (Norme 2120) et le contrôle de l'organisation (Norme 2130).

Cadre de référence du COSO ERM[145]- Principes n° 1 à 5 relatifs à la Gouvernance et à la culture

1. Exercer une surveillance des risques par le conseil

   Le conseil assure la surveillance de la stratégie et assume les responsabilités en matière de gouvernance pour soutenir la direction générale dans la réalisation de la stratégie et des objectifs opérationnels.

2. Définir les structures organisationnelles

   L'organisation définit des structures organisationnelles dans la perspective de la réalisation de la stratégie et des objectifs opérationnels.

3. Définir la culture souhaitée

   L'organisation définit les comportements attendus qui caractérisent la culture souhaitée par l'entité.

4. Démontrer l'engagement en faveur de valeurs fondamentales

   L'organisation démontre son engagement pour les valeurs fondamentales de l'entité.

5. Attirer, former et fidéliser des personnes compétentes

   L'organisation s'engage à développer le capital humain en adéquation avec la stratégie et les objectifs opérationnels.

[145] COSO ERM - 2017 « Le management des risques de l'entreprise Une démarche intégrée à la stratégie et à la performance »

	Direction Générale
Profil :	Directeur des services / Directeur général des services
Positionnement :	Le Directeur des services / Directeur général des services est en charge des services administratifs de la collectivité sous l'autorité directe du président de l'Exécutif.
Missions :	Le Superviseur DG est responsable en dernier ressort de la conduite d'une démarche de gestion prévisionnelle des risques à l'échelle de la collectivité. Il définit les risques faisant l'objet d'un risque prioritaire, en considération du degré de vulnérabilité de la collectivité à leur égard et en tenant compte de toute autre considération particulière ; le cas échéant, il en établit la liste après avis du comité des risques. Il est garant de la mise en place de mesures de maîtrise proportionnées en réponse aux principaux risques identifiés. Il veille également à la définition de l'appétence au risque de la collectivité, en accord avec les vœux du président et de l'Exécutif. Il s'assure que les arbitrages pris à cet égard sont de nature à garantir la continuité de service et à permettre la réalisation des objectifs du projet de mandat. En conséquence, il doit être en mesure de fournir en permanence une assurance raisonnable sur la bonne gestion de la collectivité et sa capacité à répondre efficacement à toute menace interne ou externe présentant un degré de crédibilité minimal. Il est tenu de fournir cette assurance à l'Exécutif ainsi que, le cas échéant, à toute autre autorité habilitée, à l'image de la Commission européenne au titre de la mise en œuvre de financements de la politique européenne de cohésion qui se trouveraient confiés à la collectivité.

	Gouvernance hors Direction Générale
Profil :	Président de la collectivité, membre de l'Exécutif, autres élus ou tout membre du comité des risques ou du comité d'audit.
Positionnement :	Les membres de la Gouvernance appartiennent de manière générale à la collectivité. Elle peut prendre une forme collégiale ou se réduire à une seule personne. Selon les cas, il s'agit de l'équipe de direction et/ou d'élus en charge du pilotage des fonctions support, notamment au regard de la politique de gestion des risques ou plus généralement des politiques de contrôle et d'audit. De manière complémentaire, la Gouvernance peut être étendue à des personnalités extérieures appelées à participer au comité des risques ou au comité d'audit.
Missions :	La Gouvernance est consultée sur toute question touchant l'amélioration des processus de management des risques et de contrôle de la collectivité. A cet effet, elle est amenée à formuler des recommandations et éventuellement à prendre toute décision utile dans les domaines suivants : ▪ Orientations stratégiques et opérationnelles de la politique de management des risques ▪ Programmation et suivi des campagnes de contrôle interne et, le cas échéant, d'audit interne ▪ Mise en place d'une gestion efficace des performances des moyens de maîtrise déployés ▪ Promotion des règles d'éthique et des valeurs appropriées. La Gouvernance a ainsi vocation à être associée à la définition de l'appétence aux risques de la collectivité. Elle est de même informée des observations des audits externes et s'assure de la mise en œuvre effective de leurs recommandations éventuelles.

Fiche technique 9

Profils engagés dans une démarche de management et de maîtrise des risques - Acteurs en charge des trois lignes de maîtrise

Le tableau ci-dessous présente les profils engagés dans une démarche assurantielle ainsi que leur positionnement au sein de la collectivité.

Dispositif de maîtrise des risques	**Profils identifiés**	**Positionnement au sein de la collectivité**
1ère ligne	**Contributeur(s) métier** (*)	Cadre de proximité / Agent support ou Agent opérationnel en charge d'un processus métier
1ère ligne	**Responsable(s) de domaine / Référent risque**	Cadre intermédiaire / Directeur général adjoint / Directeur
2ème ligne	**Manager des risques**	Responsable de la cartographie des risques & coordonnateur de la démarche
1ère ligne / 2ème ligne	**Référent contrôle interne**	Responsable du contrôle interne
3ème ligne	**Responsable audit interne**	Responsable de l'audit interne
	Responsable audit externe	Responsable de l'audit externe / Régulateur habilité

Des Fiches de poste doivent être établies en appui de recrutements ou de charge de mission internes.

Pour la mise en œuvre d'une démarche assurantielle, trois fiches de poste sont proposées :

- manager des risques ;
- responsable du contrôle interne ;
- responsable de l'audit interne.

Ces postes doivent être positionnés de manière à permettre et légitimer une action transversale sur l'ensemble des services de la collectivité et ses éventuels organismes associés.

	Contributeurs métier
Profil :	Cadre de proximité / Agent support ou Agent opérationnel en charge d'un processus métier. Le manager des risques est habilité à désigner plusieurs contributeurs métier au sein de la collectivité, en accord avec leur hiérarchie de rattachement respective. Selon la configuration de la cartographie des risques initialement arbitrée, les contributeurs métier auront la charge d'un processus métier couvrant un ou plusieurs dispositif(s), d'une thématique transverse ou de tout autre secteur d'activité particulier.
Positionnement :	Le ou les contributeur(s) métier occupent des fonctions opérationnelles concourant à la mise en œuvre des politiques de la collectivité. Ils peuvent également être chargés de fonctions support de type technique ou réglementaire en appui aux agents dédiés aux tâches opérationnelles.
Missions :	Le ou les contributeur(s) métier sont responsable de l'identification de l'ensemble des risques rattachés à leurs champs d'activité respectifs. Ils procèdent à l'inventaire de ces risques selon les indications données par le manager des risques et conduisent le chantier en étroite concertation avec celui-ci. Pour chaque risque identifié, ils déterminent un degré d'impact, de probabilité et de maîtrise. Ils mettent en place des outils de reporting appropriés pour vérifier le degré d'impact et de probabilité attachés à chaque risque. Le cas échéant, ils modifient et ajustent ces valeurs au regard des observations réalisées au fil de l'eau. De même, ils réalisent des auto-contrôles réguliers pour mesurer la maîtrise des risques identifiés. Ces auto-contrôles sont constitutifs de la première ligne de maîtrise des risques de la collectivité. Selon les résultats obtenus, ils effectuent tout ajustement nécessaire et en tant que de besoin réévaluent le degré de maîtrise pris en compte pour l'exercice de cartographie. Ils participent à l'amélioration de la maîtrise des risques en contribuant à la construction, à la mise en œuvre et au suivi du plan d'action d'amélioration.

	Responsables de domaines - Référents risques
Profil :	Cadre intermédiaire / Directeur général adjoint / Directeur.
Positionnement :	Le ou les responsable(s) de domaine occupent une position hiérarchique intermédiaire entre les Contributeurs métier et la Direction générale.
Missions :	Le ou les responsable(s) de domaine encadrent les travaux menés par les Contributeurs métier positionnés dans leur périmètre hiérarchique. A ce titre, ils supervisent l'ensemble de leurs saisies et se portent garants auprès de la Direction générale de la conformité des informations données. Un Responsable de domaine peut être également exercer les fonctions de Contributeur métier pour une part des activités situées dans son champ de responsabilité

	Manager des risques
Profil :	Responsable du déploiement du management des risques à l'échelle de la collectivité Celui-ci peut être recruté *ad hoc*. A défaut, cette mission peut être confiée à un cadre en charge de fonctions support.
Positionnement :	Le manager des risques est positionné dans l'organigramme de la collectivité de telle manière que soit garantie la transversalité de sa mission.
Missions :	Il est en charge de la conception et du déploiement de la politique de management des risques de la collectivité. A cet effet, il propose un schéma d'architecture pour assurer une couverture efficace des activités de la collectivité et, le cas échéant, de ses organismes associés. Il sollicite les arbitrages nécessaires à l'évaluation et à la formalisation de l'appétence aux risques de la collectivité. Conformément à ces lignes de partage, il s'assure que l'ensemble des agents ayant part à la réalisation et à l'actualisation de la cartographie des risques y contribuent effectivement et remplissent avec exactitude les tâches qui leur reviennent. Il est ainsi garant de la fiabilité et de la cohérence de la totalité des données renseignées et rend compte de la qualité des informations décisionnelles fournies.

Exemple de Fiche de Poste

Chargé de mission / Responsable Management des risques (1/2)

Raison d'être du poste

Compte tenu de la densité des services publics rendus aux usagers par la collectivité et de la nécessité d'apporter une réponse aux obligations ou recommandations réglementaires (ex : Fonds Social Européen, déontologie, anticorruption, …), la gestion des risques est un enjeu stratégique de la collectivité.

Pilote de la démarche globale, le chargé de mission management des risques contribue ainsi à la sécurisation (administrative, financière, juridique, …) de la collectivité, à l'amélioration continue et à la garantie de continuité du service public rendu à l'usager.

Missions

Le chargé de mission en management des risques veillera à identifier les points de vulnérabilité de la collectivité et évaluer les risques encourus (techniques, financiers, juridiques…) ainsi que leurs conséquences.

Il conseillera également les directions métier sur les mesures à prendre en compte afin de limiter les risques identifiés mais aussi en matière de gestion de crise.

Ses tâches se déclinent comme suit.

1. Concevoir, mettre en œuvre et animer la démarche de gestion des risques

- Définir les démarches de gestion des risques a priori (analyses de risques, sécurisation de processus métiers, risques majeurs) et a posteriori (analyse d'évènements indésirables) en lien avec la stratégie de la collectivité ;
- Fournir à la Direction Générale une vision globale sur la perception par les directions métiers de leurs risques et de leur maîtrise ;
- Assurer le pilotage de l'activité (alimentation de tableaux de bord, comitologie…) ;
- Réaliser un bilan des actions mises en place et des problèmes rencontrés ;
- Apporter un support méthodologique à l'organisation de la gestion de crise.

…/…

Exemple de Fiche de Poste

Chargé de mission / Responsable Management des risques (1/2)

Les tâches suivantes lui incombent également.

2. Accompagner les directions métiers pour l'identification et la maîtrise de leurs risques

- Identifier, analyser, évaluer et hiérarchiser les risques selon différentes approches (activités, processus, systèmes d'informations, outils de production, évènements, …) ;
- Organiser les ateliers d'identification et de hiérarchisation des risques avec les directions métiers ;
- Déterminer les plans d'actions de maîtrise des risques identifiés et suivre leurs réalisations ;
- Mesurer l'efficacité des actions mises en œuvre et alerter les directions métier sur les risques majeurs et les anomalies dans le suivi des plans d'actions.

Le chargé de mission management des risques rendra également compte des travaux suivants.

3. Être garant de la méthode de management des risques et force de proposition de la démarche

- Concevoir et actualiser le référentiel de management des risques (glossaire, méthodes, rôles) ;
- Développer et diffuser la culture de management des risques (communication, sensibilisation) ;
- Veille technique et juridique (méthodes, réglementation, innovations, expérimentations…) ;
- Participation active et animation de réseaux professionnels ;
- Apporter une expertise et proposer des arbitrages de la Direction Générale ;
- Assurer le suivi des décisions de la Direction Générale en lien avec les directions métier.

Pour mener à bien ses missions, le chargé de mission management des risques travaillera en transversalité et en mode projet avec l'ensemble des directions de la collectivité, mais aussi en forte interaction avec l'ensemble des compétences au sein de la collectivité.

Il s'agira en particulier de détecter les processus et situations les plus critiques susceptibles de déclencher des interventions complémentaires ciblées (audit interne, évaluation, conseil organisationnel…) en lien avec les consultants en management de la transformation et les services supports de la collectivité (conseil de gestion, affaires juridiques, finances, ressources humaines)

	Référent contrôle interne
Profil :	Responsable(s) du contrôle interne
Positionnement :	Le ou les responsable(s) du contrôle interne sont positionnés dans l'organigramme de la collectivité de telle manière qu'ils puissent appréhender de manière transversale et systémique les thématiques dont ils ont la charge.
Missions :	Le ou les Responsable(s) du contrôle interne s'assurent de la seconde ligne de maîtrise des risques de la collectivité. Conformément aux dispositions du COSO 2013 relatif au Contrôle interne[146], les vérifications menées à ce titre portent sur l'atteinte des objectifs suivants : ▪ Respect des lois, règlements, contrats ; ▪ Protection du patrimoine matériel et immatériel ; ▪ Fiabilité et intégrité des informations financières et opérationnelles ; ▪ Efficacité et efficience des opérations concourant à la mise en œuvre des politiques de la collectivité. Au sein d'une collectivité, le contrôle interne prend ainsi la forme d'un contrôle financier, de mesures de cybersécurité et de sécurité informatique, d'actions de contrôle de la qualité et de la conformité des processus métier. Dans chacun de ces périmètres, le contrôle interne vise à vérifier le degré de maîtrise des risques identifiés et, le cas échéant, à proposer les mesures correctrices requises. Les mesures correctrices demandées pourront en outre avoir une incidence sur les niveaux de probabilité et d'impact des risques concernés.

[146] Voir https://www.coso.org/Pages/ic.aspx

Exemple de Fiche de Poste

Référent du contrôle interne (1/3)

Raison d'être du poste

Le référent du contrôle interne est chargé de proposer, structurer et piloter la démarche nécessaire au déploiement du contrôle interne au sein de la collectivité.

Il participe à la diffusion d'une culture commune, fondée sur une lecture partagée des processus de production du service public et des risques associés. En veillant à la robustesse des process, comme à leur amélioration continue, il prend part à l'atteinte des objectifs stratégiques et opérationnels de la collectivité.

Le responsable du contrôle interne contribue ainsi au développement d'une culture commune fondée sur la recherche de la performance et la responsabilisation de l'ensemble des parties engagées dans la réalisation du projet de mandat / du projet d'administration de la collectivité.

Missions principales

Les missions du référent du contrôle interne s'articulent autour de trois volets.

a) Appui au déploiement de la cartographie des risques[147]

Le référent du contrôle interne s'assure du déploiement et de la mise à jour régulière d'une cartographie des risques propre à étayer le positionnement ainsi que l'étendue des dispositifs de contrôle interne.

A cet effet, il est chargé des travaux suivants :

- Accompagnement des acteurs de la démarche de maîtrise des risques dans la réalisation et l'actualisation des cartographies des risques (mise en place d'un appui méthodologique adapté aux besoins particuliers de chacune des directions concernées) ;
- Animation d'un groupe des référents de la maîtrise des risques intervenant dans les services pour accompagner l'élaboration du contrôle interne, assurer la remontée d'informations fiables et en temps utiles ainsi que le partage des bonnes pratiques ;
- Administration du système d'information de gestion des risques[148].

…/…

[147] Ce volet est conditionné à l'existence - ou non - d'un manager des risques au sein de la collectivité. Dans le cas où un manager des risques est déjà désigné, il lui reviendra prioritairement de conduire les tâches décrites.

[148] Cartographies des risques, base de données comportant le référentiel de contrôle interne, des bonnes pratiques d'identification et de maîtrise des risques, des indicateurs de suivi…

Exemple de Fiche de Poste

Référent du contrôle interne (2/3)

Le référent du contrôle interne est également chargé des travaux suivants.

b) Mise en place et coordination de dispositifs de contrôle interne couvrant les différentes missions de la collectivité

Il s'assure de l'efficacité des dispositifs de contrôle interne en phase de conception comme en phase d'exécution.

Il réalise ainsi des plans de test ciblés et veille à la mise en œuvre effective des actions correctives éventuellement requises.

A cet effet, il est chargé des travaux suivants :

- Revue des dispositifs de maîtrise des risques et identification des leviers de contrôle interne pour atteindre les objectifs de maîtrise des risques ;
- Accompagnement des lignes opérationnelles et fonctionnelles concernées par la mise en œuvre d'un dispositif de contrôle interne cohérent avec les orientations définies par le comité de pilotage de la maîtrise des risques ;
- Soutien aux actions de renforcement du contrôle interne (conception/adaptation des dispositifs de contrôle interne, procédures, plans de contrôle interne, référentiels de contrôle interne, organigrammes fonctionnels…) ;
- Mise en place des outils et des indicateurs de suivi de l'efficacité du système de contrôle interne ;
- Réalisation de tests et de contrôles ciblés permettant d'évaluer la conception et la mise en œuvre des référentiels de contrôle interne[149] ;
- Suivi de la mise en œuvre des plans d'action en réponse à tout dysfonctionnement constaté.

c) Missions transverses

Le référent du contrôle interne est garant de la mise en place d'une dynamique de progrès continu visant au renforcement de la performance au sein de la collectivité et au développement d'une organisation apprenante apte à tirer le meilleur parti de l'ensemble des informations internes et externes disponibles.

…/…

[149] Par exemple en testant la mise en œuvre d'activités de contrôle ou de plans de résolution de défaillances

Exemple de Fiche de Poste

Référent du contrôle interne (3/3)

Au titre de ses missions transverses, le référent du contrôle interne s'acquitte des tâches suivantes :

- Participation aux instances de coordination avec les autres acteurs de la deuxième ligne de maîtrise des risques (risques financiers, juridiques, systèmes d'information…) ;
- Reporting auprès des organes dirigeants, notamment au comité d'audit, du niveau de maîtrise des risques et des contrôles ;
- Proposition d'axes d'amélioration pour un usage managérial du contrôle interne ;
- Sensibilisation de l'encadrement et des agents aux enjeux et modalités de réalisation du contrôle interne, notamment au moyen de formations et de conférences ou au travers de publications et supports créés *ad hoc* ;
- Conduite de travaux de benchmarking en vue de l'éventuelle réutilisation et adaptation des bonnes pratiques observées en dehors de la collectivité ;
- Consolidation et exploitation de toute information pertinente (auto-évaluations, remontées d'indicateurs par les animateurs du contrôle interne).

	Responsable de l'audit interne
Profil :	Responsable(s) de l'audit interne
Positionnement :	Le responsable de l'audit interne est positionné dans l'organigramme de la collectivité de manière à assurer son indépendance fonctionnelle et à garantir l'objectivité des avis rendus. A cet effet, il est recommandé de le rattacher directement à l'Exécutif ou à défaut à la Direction générale.
Missions :	Le responsable de l'audit interne est chargé de la troisième et dernière ligne de maîtrise des risques de la collectivité, selon les modalités fixées par le Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP)[150] . A cet effet, il lui revient de réaliser des travaux d'audit sur les risques jugés critiques de la collectivité afin de vérifier l'efficacité et l'efficience des mesures de maîtrise mises en place et, dans le cas où des dysfonctionnements sont constatés, de proposer toute action correctrice requise. Les travaux d'audit peuvent en outre porter sur des risques déjà reconnus comme insuffisamment maîtrisés ; ils visent alors à l'élaboration de recommandations tendant à diminuer le degré de vulnérabilité de la collectivité dans le périmètre concerné. Ces investigations portent prioritairement sur les dispositifs existants de contrôle interne. Elles permettent de construire une opinion d'audit sur la qualité de gestion de la collectivité et sa capacité à atteindre les objectifs du projet de mandat. Selon un échéancier fixé, le responsable de l'audit interne communique cette opinion à la Direction générale et au président de la collectivité. Pour la conduite de ses travaux et le cas échéant, il peut prendre appui sur un Comité d'audit placé en principe sous la présidence d'un représentant de l'Exécutif et éventuellement ouvert à des personnalités extérieures qualifiées.
Pour creuser la question…	Voir la Fiche de poste AUDITEUR.TRICE INTERNE établie par le CNFPT (N° 07/A/01)[151]

[150] Voir notamment les dispositions de la Norme 1110 du CRIPP

[151] Ce document est téléchargeable sur le lien suivant :
https://www.cnfpt.fr/evoluer/lemploi-fpt/le-repertoire-des-metiers/metier/details/A1B-04

Exemple de Fiche de Poste

Responsable de l'audit interne (1/3)

Raisons d'être du poste

Dans un contexte marqué par de fortes mutations et de nombreuses incertitudes, le responsable de l'audit interne est investi d'un rôle d'assurance et de conseil visant à consolider la gestion des risques de la collectivité et à optimiser les moyens de maîtrise et de contrôle existants.

Ce faisant, le responsable de l'audit interne est garant de la bonne gestion de la collectivité, de la correcte maîtrise des risques majeurs identifiés et aussi de la fiabilité des données propres à éclairer les choix stratégiques de la collectivité.

Il est ainsi chargé de questionner les dispositifs internes de la collectivité de manière à :

- Evaluer la performance des processus afin d'identifier les sources potentielles d'efficience ;
- Mesurer leur conformité au regard des référentiels applicables, tant externes que propres à la collectivité ;
- Sensibiliser la gouvernance et l'encadrement en matière de gestion des risques et de contrôle interne, et les informer et/ou alerter sur le degré de maîtrise de leurs opérations ;
- Conseiller la gouvernance et l'encadrement pour leur permettre d'optimiser leurs processus de gestion des risques, de contrôle et de gouvernance et prévenir ainsi les dysfonctionnements ;
- Favoriser la diffusion des bonnes pratiques et formuler des recommandations visant à améliorer l'efficacité du service public.

Dans ce cadre, il est habilité à intervenir dans l'ensemble des directions et services de la collectivité ainsi que de ses satellites et peut faire appel en tant que de besoin aux compétences complémentaires des services supports ou d'organismes extérieurs.

A cette fin, l'accès sans restriction à l'ensemble des informations nécessaires à la bonne conduite de ces opérations d'audit est garanti par la Direction générale.

Dans le cadre d'une programmation [pluriannuelle] établie par le Comité d'audit et des risques, le Responsable de l'audit interne est amené à piloter des missions d'analyse et de diagnostic dans divers domaines spécifiquement circonscrits pour chacune d'elles.

Ces travaux font l'objet de rapports étayés en vue de l'obtention des améliorations recherchées.

…/…

Exemple de Fiche de Poste

Responsable de l'audit interne (2/3)

Missions principales

Le Responsable de l'audit interne a vocation à mettre en œuvre ses compétences dans la stricte application du cadre déontologique de l'audit interne, mis à jour de manière permanente.

A ce titre, il est en charge de :

- L'organisation des missions d'audit, en fonction du programme pluriannuel d'audit

  Tâches associées : Analyse des risques, à partir de la cartographie des risques établie et mise à jour par la direction, planification des programmes d'intervention, et mobilisation des ressources nécessaires, alerte de l'autorité territoriale sur les points de vigilance et les dysfonctionnements éventuels relevés, et retour sur les conditions d'accès aux informations nécessaires, rédaction d'un rapport d'activité sur la réalisation du programme d'audit)

- De la conduite opérationnelle des missions d'audit

  Tâches associées : conception et mise en place de dispositifs d'investigation et de vérification, recueil et analyse des éléments et informations nécessaires, conduite d'entretiens, mise en œuvre de techniques d'analyse, évaluation de la performance du contrôle interne, contrôle de l'application des méthodes et procédures de contrôle interne, contrôle de la régularité des états financiers, analyse des organisations et processus métiers

- De l'exploitation et la communication des résultats d'audit

  Tâches associées : formalisation, restitution et proposition des conclusions des rapports d'audit dont il a la charge en veillant à la mise en pratique effective d'une procédure contradictoire, formulation et explicitation des recommandations d'amélioration et/ou de correction, contrôle de l'effectivité de la mise en œuvre des plans d'action, suivi et synthèse de l'activité d'audit.

- Du suivi de la mise en place des recommandations préconisées.

En dehors des missions d'audit réalisées en interne, l'auditeur est amené à :

- accompagner et assurer le suivi des missions d'audit réalisées par des prestataires externes ;
- contribuer à la mise en place de la cartographie des risques de nos collectivités et à son actualisation périodique, sous réserve des responsabilités de premier rang incombant dans ce domaine au manager des risques et au contrôleur interne.

…/…

Exemple de Fiche de Poste

Responsable de l'audit interne (3/3)

Activités secondaires

Afin de valoriser et développer ses compétences, le Responsable de l'audit interne veillera à :

- Identifier les domaines d'expertise utiles à la bonne conduite des missions d'audit interne afin de se former ;
- Recueillir et diffuser une documentation professionnelle et règlementaire (veille règlementaire et sectorielle des pratiques professionnelles) ;
- Participer aux réunions organisées avec les entités spécialisées ;
- Partager ses compétences et expériences au sein de la direction.

	Responsable de l'audit externe
Profil :	Toute autorité d'audit ou de régulation extérieure à la collectivité (juridictions financières par exemple)
Positionnement :	Il peut s'agir notamment de la Chambre régionale des comptes ou de toute autre autorité habilitée à vérifier la correcte application de toute réglementation spécifique, telle que la Commission nationale de l'informatique et des libertés (CNIL) en charge de la vérification de la correcte application des dispositions du Règlement général pour la protection des données[152.] Pour les collectivités qui se sont vu confier la mise en œuvre de programmes européens, on peut également citer les services de la Commission européenne ou de la Cour des comptes européenne en charge de l'audit des financements alloués. En outre, dans le cadre de la démarche expérimentale de certification des comptes de la collectivité[153,] un Commissaire aux comptes désigné pourra mener des audits externes pour fonder sa décision finale.
Missions :	Une autorité d'audit externe donne un avis sur la correcte application par la collectivité des différentes obligations auxquelles elle est astreinte, dans son champ d'investigation particulier. En cas de manquement constaté, elle est généralement habilitée à prononcer des sanctions d'ordre financier ou autre.

[152] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[153] Expérimentation menée sur le fondement de la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République (loi NOTRe)

Fiche technique 10

Risques le plus fréquemment rencontrés et exemples d'univers de risques dans différents types de collectivités

Pour construire sa cartographie des risques, une collectivité peut se référer à la nomenclature issue du référentiel COSO 2 ERM dans la mesure où elle offre un socle robuste et évolutif pour développer des Dispositifs de contrôle interne répondant à ses objectifs prioritaires.

Le référentiel COSO 2 ERM distingue ainsi les quatre catégories de risques suivants :

- les risques stratégiques liés à la non-atteinte des objectifs politiques du mandat ;
- les risques opérationnels liés à la défaillance de processus métier du fait de l'inadaptation des moyens disponibles et/ou de circuits de traitement inappropriés ;
- les risques comptables et financiers liés à une réduction de la marge de manœuvre budgétaire de la collectivité, à des pertes financières (non-encaissement de recettes et/ou paiement de montants indus) à l'inexactitude des comptes présentés à l'Exécutif ;
- les risques réglementaires liés à la non-application de la législation en vigueur.

Selon le contexte de chaque collectivité, d'autres catégories de risques peuvent y être ajoutés, tels que notamment :

- des risques RH liés à la perte de compétences clés, à une démotivation des effectifs ; à un *turn-over* excessif ;
- des risques SI liés à une utilisation déficiente des ressources informatiques ;
- des risques de fraude liés à la possibilité que soient commis au sein de la collectivité des actes contraires à la probité[154] ;
- des risques exogènes susceptibles d'affecter brutalement et durablement le fonctionnement de la collectivité.

En faisant apparaître distinctement ces catégories de risques, une collectivité manifeste son attention particulière aux thématiques considérées.

Ainsi sur une base commune minimale, on trouvera autant de cartographies différentes qu'il y a de collectivités et chacune d'entre elles a vocation à s'inscrire dans une histoire qui lui est propre.

[154] Voir Fiche technique n° 2

Proposition de liste de risques par catégorie

A. Exemple d'univers des risques donné par l'AMRAE

L'univers des risques proposé par l'AMRAE ne répond que pour partie aux spécificités des collectivités territoriales ; il peut cependant être conservé comme un modèle de référence pour les travaux de cartographie qu'il leur appartient de mener.

<table>
<tr><th colspan="3">Risques externes</th></tr>
<tr><td colspan="3">Concurrence - Lobbying social - Législation - Catastrophes naturelles - Réglementation - Crise sur marché clé - Terrorisme - Relations avec les parties prenantes - Partenaires - Innovation technologique - Etc…</td></tr>
<tr><th colspan="3">Risques internes</th></tr>
<tr><td colspan="3">Risques stratégiques</td></tr>
<tr><td colspan="3">Labelling - Propriété intellectuelle - Stratégie de développement - Business model - Canaux de distribution portefeuille - Perte de part de marché - Stratégie marketing - Profitabilité - Fusion & acquisition - Intégration - Gouvernance - Communication externe - Etc…</td></tr>
<tr><td>Risques opérationnels</td><td>Capital humain</td><td>Conformité</td></tr>
<tr><td rowspan="4">Santé et sécurité - Connaissance, savoir-faire - Développement - Cycle de vie des produits - Pollution - Accident majeur - Distribution - Arrêt de l'activité - Dommages aux tiers - Défaillance équipement critique - Qualité produit/service - Carence de fournisseurs - Dommages aux actifs - Capacité - Carence énergie - Interdépendance entre sites - Erosion marque - Bâtiments</td><td>Externalisation - Personne clé - Communication - Compétences - Gestion du changement / recrutement - Accident - Exposition dangereuse - Etc…</td><td>Législation & réglementation - Contractuelle - Juridique - Communication financière</td></tr>
<tr><td>Systèmes d'information (informatique)</td><td>Gouvernance et intégrité</td></tr>
<tr><td>Technologie - Infrastructure - Intégrité - Accès - Maintenance - Disponibilité - Confidentialité - Dépendance - Externalisation - Pertes de données</td><td>Leadership - Délégation - Limites - Autorité - Performances incitatives - Fraude - Actes illégaux - Usage illégal - Ethique - Image de marque</td></tr>
<tr><td colspan="2">Finances</td></tr>
<tr><td colspan="2">Taux d'intérêts - Liquidité - Risque crédit - Pension - Risque de change - Management finance (budget, forecast, pricing, impôts…) - Dépréciation d'actifs - Provisions - RC</td></tr>
</table>

B. Arborescence proposée dans le cadre d'enquêtes annuelles

Pour la construction de leur cartographie des risques, les collectivités peuvent également s'inspirer de la classification des risques proposée dans le « Baromètre de la gestion globale des risques au sein des collectivités »[155]

Risques stratégiques, de gouvernance et d'image (STRAT)

- Echec / retard / surcoûts d'un projet clé (aménagement, infrastructure…)
- Echec d'un chantier interne de modernisation ou d'un projet de réforme (transformation, organisation…)
- Dysfonctionnement majeur de la chaîne de décision (articulation entre sphère administrative et politique)
- Crise médiatique / dénigrement (élus, collectivité…)
- Baisse réelle ou perçue de l'attractivité du territoire (habitants, entreprises…)
- Mutation (institutionnelle, technologique, sociétale…) au sein du territoire non ou mal anticipée
- Défaillance d'un satellite / d'une concession / d'une délégation de service public

Risques financiers (FIN)

- Dérive budgétaire (perte de revenus, augmentation incontrôlée des coûts, dette…)
- Difficultés majeures / tensions en matière de financement (accessibilité, coûts)
- Erreur / défaut de fiabilité des informations comptables et financières

Risques humains (RH)

- Accident majeur dans un établissement (incendie, effondrement…)
- Accident majeur impliquant un usager du service public (voirie, accident corporel…)
- Comportement inapproprié d'un agent vis-à-vis d'un usager (violence, maltraitance, abus de droit…)
- Accidents du travail / maladies professionnelles (y compris risques psychosociaux)
- Tensions sur des catégories de personnel / des compétences critiques (recrutements…)
- Conflit social (grève, blocage…)
- Absentéisme
- Perte brutale d'un collaborateur clé

Risques opérationnels (OPER)

- Défaillance d'un fournisseur clé (gardiennage, restauration, systèmes d'information…)
- Défaillance critique / indisponibilité des systèmes d'information (paye, serveur de données…)
- Perte, vol ou diffusion d'informations sensibles / confidentielles
- Occupation illicite de l'espace public ou d'immeuble de la collectivité

[155] Ce baromètre est publié par Arengi en partenariat avec la CIAT. La présente classification figure dans sa première édition (2013)

Risques opérationnels (OPER) - Suite

- Interruption durable d'une mission de service public (eau, assainissement, traitement des ordures…)
- Fraude interne (agent) ou fraude externe (usagers, autres)
- Erreur / délai dans l'attribution / l'instruction d'une demande d'aide financière

Risques exogènes (EXO)

- Actes de terrorisme
- Risques naturels / climatiques (tempêtes, inondations, mouvements de terrain, incendies de forêts…)
- Risques technologiques (risques industriels, transport de matières dangereuses, risque nucléaire…)
- Risques sanitaires (pandémie, canicule, ondes électromagnétiques, intoxication…)
- Augmentation de l'insécurité (émeutes urbaines, criminalité…)

Risques juridiques / réglementaires (REGL)

- Non-respect de la réglementation / irrégularité juridique des actes
- Dysfonctionnement / erreur dans la passation d'un marché public
- Evolution défavorable / non anticipée d'une réglementation

Les 10 risques prioritaires des collectivités

Résultats d'un sondage réalisé en appui de cette nomenclature

	Toutes collectivités confondues	Catégorie
①	Accident du travail / maladies professionnelles	RH
②	Défaillance d'un satellite, d'une concession, d'une DSP	STRAT
③	Echec d'un chantier de modernisation ou d'un projet de réforme	STRAT
④	Absentéisme	RH
⑤	Défaillance critique / indisponibilité des systèmes d'information	OPER
⑥	Tensions sur des catégories de personnel / perte de compétences critiques	RH
⑦	Accident majeur dans un établissement (incendie, effondrement	EXO
⑧	Fraude interne (agent) ou fraude externe (usager, autres…)	OPER
⑨	Echec / retard / surcoût d'un projet clé (aménagement, infrastructure…)	STRAT
⑩	Mutation (institutionnelle, technologique, sociétale…) non ou mal anticipée	STRAT

Fiche technique 11

Outils & méthodes d'évaluation des risques présentés dans la Norme ISO 31000 relative au management des risques

La Norme ISO 31000-2018 relative au management des risques décrit 31 outils & méthodes pour l'identification et l'évaluation des risques au sein d'une organisation[156].

Ces outils & méthodes répondent à des finalités différentes et couvrent des périmètres bien distincts.

Comme toute organisation, une collectivité territoriale est appelée à utiliser simultanément ou consécutivement plusieurs de ces instruments dans le cadre du déploiement d'une fonction de management des risques couvrant l'ensemble de ses activités et des politiques menées.

Au regard des étapes nécessaires à la conduite d'une telle démarche, il paraît à propos de les répartir selon quatre catégories.

Une **première catégorie** comprend les outils & méthodes visant à la fabrication d'un consensus éclairé au niveau technique.

> Il s'agit de méthodes de préparation et d'appui aux travaux d'experts sollicités pour la description de processus métier, l'identification et l'évaluation des risques afférents, l'identification des moyens de maîtrise qui y répondent. Il apparaît en effet que l'attention portée aux questions posées et aux modalités de conduite des entretiens renforce sensiblement la fiabilité des informations recueillies.

Une **seconde catégorie** comprend les outils & méthodes visant au dépistage des causes, à l'identification des conséquences et à la modélisation des process.

> On y trouve les techniques de représentation et de classification ayant pour objet l'analyse de scénario, l'analyse fonctionnelle ou l'évaluation des contrôles associés aux risques identifiés.

Une **troisième catégorie** comprend les outils & méthodes visant à la conduite de revues d'éléments disponibles, à la quantification de données et à des calculs de probabilités.

> Elle réunit principalement des méthodes de recherche et des méthodes statistiques visant à déterminer la probabilité de risques particuliers.

Une **quatrième catégorie** comprend les outils & méthodes visant au pilotage et à la préparation des arbitrages soumis à la gouvernance.

> Ce dernier ensemble regroupe les supports décisionnels proposés à la gouvernance pour identifier les risques prioritaires, s'assurer du degré de maîtrise obtenu et déterminer l'appétence au risque de la collectivité en particulier sur des questions sensibles touchant à la sécurité des personnes, à la lutte contre la fraude etc…

[156] Norme ISO 31000 de Juin 2018 - Management du risque - Lignes directrices

Selon cette approche, les 31 outils & méthodes décrits dans la Norme ISO 31000 peuvent se partager comme suit.

3 outils & méthodes visent à la fabrication d'un consensus éclairé au niveau technique

- Brainstorming- B 01
- Entretiens structurés ou semi-structurés - B 02
- Techniques Delphi - B 03

16 outils & méthodes visent au dépistage des causes, à l'identification des conséquences et à la modélisation des process

- Analyse préliminaire du danger - B 05
- Etudes de danger et d'exploitabilité (HAZOP) - B 06
- Evaluation des risques environnementaux / Evaluation de la toxicité - B 08
- Structural « What-if » Techniques - SWIFT - B 09
- Analyse d'impact sur l'activité - B 11
- Analyse de causes profondes - B 12
- Analyse des modes de défaillance et de leurs effets (AMDE) / Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) - B 13
- Analyse par arbre de panne - B 14
- Analyse par arbre d'événements - B 15
- Analyse causes-conséquences - B 16
- Analyse des causes et de leurs effets - B 17
- Layer of Protection Analysis (LOPA) - B 18
- Analyse de fiabilité humaine - B 20
- Analyse « nœud papillon » - B 21
- Maintenance basée sur la Fiabilité - B 22
- Analyse des conditions insidieuses (analyse transitoire) - B 23

6 outils & méthodes visent à la conduite de revues d'éléments disponibles, à la quantification de données et à des calculs de probabilités

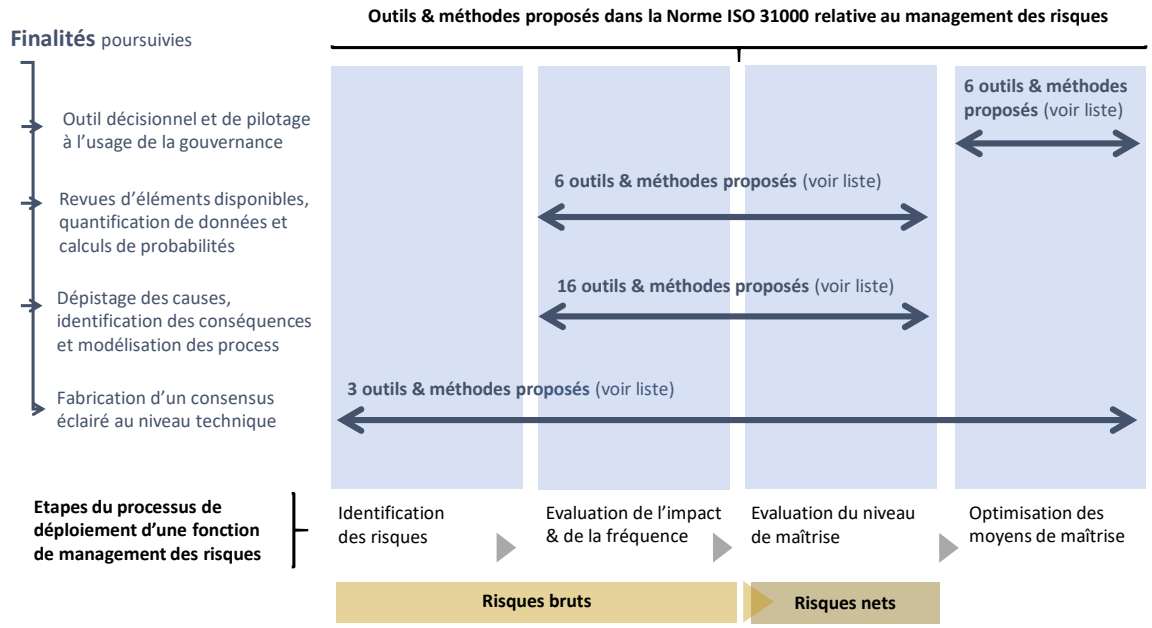
- Listes de contrôle - B 04
- Hazard Analysis and Critical Control Points - HACCP - B 07
- Analyse de Markov - B 24
- Simulation de Monte-Carlo - B 25
- Analyse bayesienne et réseaux de Bayes - B 26
- Indices de risque - B-28

6 outils & méthodes visent au pilotage et à la préparation des arbitrages soumis à la gouvernance

- Analyse de scénario - B 10
- Arbre de décisions - B 19
- Courbes FN - B 27
- Matrice conséquences/ probabilité - B-29
- Analyse coût/bénéfice - B-30
- Analyse de décision à critères multiples (ADCM) - B-31

> Pour plus de précisions, voir le tableau synthétique joint et les deux **Annexes** jointes

Utilisation des outils & méthodes proposés dans la norme ISO 31000 aux différentes étapes du déploiement d'une fonction de management des risques



Pistes pour la mise en place d'un cadre méthodologique propre à soutenir la création d'une fonction de management des risques et son installation dans la durée

En amont de la création effective d'une fonction de management des risques, une collectivité peut trouver avantage à retenir et déployer au moins quatre outils & méthodes issus de la Norme ISO 31000 et de les répartir de manière à couvrir chacune des catégories susvisées, à raison d'un dispositif ou plus par catégorie.

Ce travail préalable d'analyse doit permettre de créer un socle opérationnel fortement adossé au référentiel national applicable et de sécuriser la démarche engagée sur le moyen et long terme.

Il convient de le mener à bien de manière collégiale afin de solliciter les différentes ressources expertes de la collectivité et de créer les conditions d'une dynamique collective dès les commencements du projet.

Pour ce faire, il paraît approprié de créer un groupe exploratoire composé de représentants de l'ensemble des fonctions support et des directions métier de la collectivité ayant part au management des risques.

Sur la base de l'offre existante, ce groupe doit être à même de tester et identifier un nombre resserré d'outils & méthodes aisément combinables et proportionnés aux moyens de la collectivité qui garantiront la bonne fin du chantier engagé.

Les outils & méthodes ainsi retenus devront être mis en œuvre dans un calendrier échelonné conduisant à la généralisation de la démarche et à la création des mécanismes de régulation nécessaires à sa pérennité.

Par ailleurs, la collectivité ne doit pas s'interdire de recourir ponctuellement à des outils & méthodes additionnels, dans la mesure où il apparaitra que leur utilisation permet de répondre plus adéquatement à des besoins spécifiques qui se manifesteront au fil de l'eau.

Les collectivités qui ne disposeraient pas en interne de la technicité requise pour étayer le choix des outils & méthodes les mieux appropriés et/ou pour documenter la mise en application des solutions retenues ont également la possibilité de travailler en réseau afin de mutualiser et optimiser la ressource disponible.

Tableau synthétique des outils & méthodes pour l'évaluation des risques

Source

Norme ISO 31000 relative au management des risques - Annexe A - Tableau A-1 « Applicabilité des outils utilisés pour l'évaluation des risques » - Annexe B - Techniques d'évaluation des risques

Légende

1) Catégorie

Outils & méthodes visant à la fabrication d'un consensus éclairé au niveau technique

Outils & méthodes visant au dépistage des causes, à l'identification des conséquences et à la modélisation des process

Outils & méthodes visant à la revue d'éléments disponibles, à la quantification de données et à des calculs de probabilités

Outils & méthodes visent au pilotage et à la préparation des arbitrages soumis à la gouvernance

2) Documents de référence associés

Pour les outils & méthodes signalés par un soulignement des caractères, des documents de référence sont proposés en accompagnement - Voir leur liste à la suite de ce tableau

Annexes

Deux annexes jointes :

> **Annexe 1** - Techniques de brainstorming

> **Annexe 2** - Diagramme Cause/Effet ou diagramme d'Ishikawa

> **Annexe 3** - Visualisation de l'arbitrage coût/avantage d'une maîtrise des risquesMéthode ALARP (As low as reasonably practicable)

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 01	Brainstorming	✓✓		Le brainstorming consiste à stimuler et encourager une conversation libre au sein d'un groupe de personnes compétentes afin d'identifier les modes de défaillance potentiels et les dangers, risques, critères de sélection et/ou options de traitement associés. (Voir Annexe 1) Le brainstorming peut être formel ou informel. Il peut également être utilisé avec d'autres méthodes d'évaluation des risques décrites ci-dessous.
B 02	Entretiens structurés ou semi-structurés	✓✓		Dans un entretien structuré, un ensemble de questions préparées sont posées aux personnes interrogées à partir d'une feuille de suggestions, les encourageant à aborder une situation selon différents points de vue et à identifier les risques selon ces perspectives. Un entretien semi-structuré est similaire mais offre plus de liberté de conversation pour explorer les questions soulevées.
B 03	Techniques Delphi	✓✓	Analyse des causes et de leurs effets (B-17)	La technique Delphi est un mode opératoire permettant d'obtenir un consensus fiable sur les avis d'un groupe d'experts. Chaque expert est invité à exprimer son avis, de manière individuelle et anonyme, tout en ayant accès aux avis de ses homologues au fur et à mesure de l'avancée du processus.
B 04	Listes de contrôle	Σ		Les listes de contrôle répertorient les dangers, risques ou défaillances de contrôles qui ont été développés, en général par expérience, à la suite d'une précédente évaluation des risques ou des défaillances déjà survenues. Une liste de contrôles peut être utilisée pour identifier les dangers et les risques ou pour évaluer l'efficacité des contrôles. Elle peut être utilisée dans le cadre d'autres techniques d'évaluation des risques. Cette méthode repose sur l'observation et peut être aisément appréhendée, elle présente toutefois l'inconvénient d'ignorer les problèmes non encore décelés.

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 05	Analyse préliminaire du danger		LOPA (B-18)	Il s'agit d'une méthode d'analyse inductive simple consistant à identifier les dangers ainsi que les situations et les événements dangereux pouvant nuire à une activité, une installation ou un système donné. Cette analyse est particulièrement pertinente en phase amont du développement d'un projet lorsque peu d'informations relatives aux détails de conception et aux procédures de fonctionnement sont disponibles.
B 06	Etudes de danger et d'exploitabilité (HAZOP)		SWIFT (B-09) Arbre d'événement (B-15) LOPA (B-18) Analyse des conditions insidieuses (B-23) Matrice conséquences/ probabilité (B-29)	Cette technique vise à identifier les risques auxquels sont confrontés les personnes, les équipements, l'environnement et/ou les objectifs d'une organisation au travers de l'examen structuré et systématique du/des produit(s), processus et mode(s) opératoire(s) afférent(s). Elle repose sur l'utilisation de mots-guides permettant de déterminer dans quelle mesure il n'est pas possible d'obtenir la conception, ou les conditions de fonctionnement attendues à chaque étape de la conception, du processus, du mode opératoire ou du système. L'exercice ainsi mené conduit à identifier les modes de défaillance d'un processus, d'un système ou d'un mode opératoire ainsi que leurs causes possibles et leurs conséquences.
B 07	Hazard Analysis and Critical Control Points - HACCP			Méthode développée dans le cadre d'un programme de santé alimentaire. Elle repose sur une revue complète des dangers susceptibles d'avoir un impact sur la qualité, la sécurité ou la fiabilité d'un produit ou sur le résultat d'un processus déterminé. L'analyse HACCP a pour but de limiter les risques en procédant à des contrôles placés tout au long du processus, au lieu de procéder à une inspection du produit fini.

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 08	Evaluation des risques environnementaux / Evaluation de la toxicité			Cette méthode a été développer pour évaluer les risques environnementaux auxquels sont exposés les végétaux, les animaux et les hommes en vue de la mise en place des mesures de maîtrise appropriées. Elle prend souvent la forme d'une analyse de cheminement permettent d'explorer les voies d'exposition d'une cible à une source de risque dans des scénarios précisément définis. Les informations provenant de l'analyse de danger et de l'analyse de l'exposition sont rassemblées afin d'estimer la probabilité de conséquences particulières lorsque les effets des cheminements sont combinés.
B 09	Structural « What-if » Techniques - SWIFT		HAZOP (B-06)	Il s'agit d'une alternative à la méthode HAZOP voulue plus accessible et simple dans son utilisation. Dans un premier temps, un facilitateur établit une revue des dangers et des risques susceptibles d'affecter chaque processus étudié sur la base de normes, de mots ou phrases à effet immédiat. Ces éléments sont examinés dans le cadre d'ateliers associant les experts concernés. Le facilitateur et l'équipe utilisent des phrases du type « Que se passerait-il si ? » en combinaison avec les invites pour déterminer l'impact des écarts par rapport aux fonctionnements et comportements normaux sur le système, l'installation, l'organisation ou le mode opératoire considéré.
B 10	Analyse de scénario			L'analyse de scénario est un modèle descriptif de la manière dont l'avenir peut se présenter qui est plus particulièrement pertinent pour la définition de la stratégie d'une organisation. Cet exercice est utile pour anticiper l'apparition de menaces et d'opportunités - notamment par extrapolation depuis le présent de scenarii potentiels - et peut s'appliquer à tous les types de risques à court et long termes. .../...

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
	Analyse de scénario (suite)			La structure de l'analyse peut être formelle ou informelle, elle aboutit à l'identification d'un éventail d'événements à venir possibles, affectés d'un coefficient de risque et d'indicateurs propres à orienter les choix de l'organisation selon la tournure des événements observés.
B 11	Analyse d'impact sur l'activité			Cette méthode vise à analyser la manière dont les principaux risques de perturbation pourraient avoir un impact sur les opérations d'une organisation puis à quantifier les aptitudes nécessaires à leur gestion. Elle repose sur l'identification des points critiques des processus-métier, des fonctions et des ressources associées ainsi que des principales interdépendances qui existent au sein de l'organisation concernée. Elle permet de déterminer les calendriers de relance des processus et des ressources de soutien au moyen de questionnaires, d'entretiens et/ou d'ateliers structurés.
B 12	Analyse de causes profondes		Arbre de panne (B-14) Analyse des causes et de leurs effets (17) Diagramme d'Ishikawa (Annexe 2)	Cette méthode prend la forme de l'analyse d'une perte majeure pour empêcher qu'elle ne se reproduise. En cas de pertes d'actifs faisant suite à différents types de défaillances, l'exercice a pour but d'identifier les causes d'origine ou racines au lieu de ne traiter que les symptômes évidents. Son champ habituel d'application comprend les enquêtes sur les accidents et de l'hygiène et la sécurité au travail ; l'analyse est confiée à un groupe d'experts et prend appui sur diverses techniques de visualisation telles que l'arbre de panne, l'analyse de Pareto ou le diagramme d'Ishikawa (voir Annexe 2).
B 13	Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)		Maintenance basée sur la Fiabilité (B-22) Analyse des conditions insidieuses (B-23) Matrice conséquences/ probabilité (B-29)	Cette méthode, orientée vers l'industrie et la production, permet d'identifier dans quelle mesure les composants, les systèmes ou les processus peuvent tomber en panne pour exécuter la conception prévue. …/…

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
	AMDEC (suite)			Elle fournit un socle de planification des essais et de la maintenance des systèmes physiques ; elle permet également de vérifier la prise compte de tous les modes de défaillance des systèmes et processus (y compris l'aspect humain) et ceci dès la phase de leur conception. Les modes de défaillance ainsi identifiés sont classés selon leur criticité en vue de la mise en place des actions correctives les mieux appropriées.
B 14	Analyse par arbre de panne		Analyse causes-conséquences (B-16) Analyse de fiabilité humaine (B-20) Analyse « nœud-papillon » (B-21) Analyse des conditions insidieuses (B-23) Indices de risque (B-28)	Cette technique permet d'identifier et d'analyser les facteurs qui peuvent contribuer à un événement indésirable spécifique (dit « événement de tête »). Les facteurs de causalité sont identifiés de manière déductive et organisés de manière logique et graphique, sous la forme d'une arborescence décrivant les facteurs de causalité (événements extérieurs associés, erreurs humaines…) et leurs relations avec la survenance de l'événement de tête. Un arbre de panne peut notamment être utilisée en phase de conception d'un système pour identifier les causes potentielles de défaillance et guider un choix parmi les différentes options possibles.
B 15	Analyse par arbre d'événements		HAZOP (B-06) Analyse causes-conséquences (B-16) Analyse « nœud papillon » (B-21) Indices de risque (B-28)	Cette méthode graphique permet de représenter les séquences d'événements mutuellement exclusifs suivant un événement initiateur en fonction des scénarios de réponse de systèmes conçus pour en limiter la propagation et les effets. Une analyse préalable est indispensable pour déterminer les événements qui engendrent le déclenchement d'un incident, ceci peut être notamment réalisé en utilisant d'autres méthodes d'analyse telles que la technique HAZOP(B-06) Chaque chemin traversant l'arbre représente la probabilité de survenance de l'événement et permet de la mesurer avec un degré optimal de précision.

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 16	Analyse causes-conséquences		Arbre de panne (B-14) Arbre d'événement (B-15)	Cette méthode est une combinaison de l'analyse par arbre de panne et de l'analyse par arbre d'événements. Il s'agit d'identifier des événements critiques et d'analyser leurs conséquences potentielles ainsi que les défaillances éventuelles des systèmes conçus pour en limiter la portée ; les causes des défaillances étudiées sont représentées en utilisant des arbres de panne. De la sorte, il est possible d'analyser les différents chemins dont dispose un système à la suite d'un événement critique et aussi d'incorporer des actions différées dans l'examen des conséquences.
B 17	Analyse des causes et de leurs effets		Techniques Delphi (B-03) Analyse des causes profondes (B-12) Diagramme d'Ishikawa (Annexe 2)	Cette méthode permet d'identifier les causes possibles d'un effet particulier, qui peut être selon les cas un objectif ou un événement indésirable. Les facteurs contributifs possibles sont recensés par un groupe d'experts et organisés en catégories générales, de telle sorte que toutes les hypothèses possibles puissent être également considérées. La représentation graphique utilise le diagramme d'Ishikawa (voir Annexe 2). Il peut être intéressant d'y associer une autre méthode d'analyse de type Delphi, brainstorming ; un parallèle peut également être tracé avec la technique d'analyse des causes profondes.
B 18	Layer of Protection Analysis - LOPA		Analyse préliminaire du danger (B-05) HAZOP (B-06)	Il s'agit d'une méthode semi-quantitative d'estimation des risques liés à un événement ou à un scénario indésirable, son objet particulier est d'analyser la robustesse des mesures et de contrôle et de limitation des risques prises en réponse. Une paire cause-conséquence est sélectionnée, puis des niveaux de protection empêchant la cause de donner lieu à la conséquence indésirable sont identifiés. …/…

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
	LOPA (suite)			Un ordre de grandeur est calculé pour déterminer sur la protection permet de réduire le risque à un niveau acceptable. Cette technique permet de déterminer le niveau de protection offert par une solution particulière ; elle peut être associée à des processus de dépistage de type « Analyse préliminaire du danger » ou HAZOP.
B 19	Arbre de décisions			Cette méthode simple permet de représenter des alternatives et des résultats de décisions de manière séquentielle. Il s'agit de sélectionner un événement initiateur ou une décision et de modéliser différents scénarios résultant d'événements et/ou décisions ultérieurs. La probabilité des événements peut être estimée ainsi que le coût ou l'utilité du résultat final du cheminement ; Les informations relatives au meilleur cheminement de décision sont celles qui produisent la valeur plus élevée (produit de toutes les probabilités conditionnelles tout au long du cheminement et de la valeur du résultat).
B 20	Analyse de fiabilité humaine		Arbre de panne (B-14)	L'objet recherché ici est l'évaluation de l'impact des comportements humaines sur les performances des systèmes. Cette méthode peut être utilisée de manière qualitative ou quantitative. Du point de vue qualitatif, elle permet d'identifier le potentiel d'erreur humaine et ses causes, de façon à réduire la probabilité d'erreurs. Du point de vue quantitatif, elle fournit des données sur les défaillances humaines dans l'analyse par arbre de panne ou d'autres causes techniques.
B 21	Analyse « nœud papillon »		Arbre de panne (B-14) Arbre d'événements (B-15)	Cette technique est un moyen schématique simple pour décrire et analyser les chemins d'un risque depuis ses causes jusqu'à ses conséquences. Elle peut être considérée comme la combinaison d'un arbre de panne permettant d'analyser les causes d'un risque particulier et d'un arbre d'événements pour l'examen de ses conséquences. …/…

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
	Analyse « nœud papillon » (suite)			En complément, le schéma proposé permet de visualiser les barrières mises en place pour prévenir ou limiter les conséquences indésirables ou éventuellement stimuler et favoriser des conséquences souhaitées (contrôles de prévention, contrôles de reprise…) Cet outil peut être associé à d'autres méthodes (de type brainstorming) pour faciliter les échanges et aider à faire avancer une réflexion commune.
B 22	Maintenance basée sur la Fiabilité		AMDEC (B-13)	Cette méthode est orientée vers la maintenance de système et de production ; elle vise à identifier les règles qu'il convient de mettre en place pour gérer les défaillances et atteindre de manière efficiente le niveau de sécurité, de disponibilité et d'économie requis pour tout type d'équipement. L'analyse menée repose sur une évaluation des risques prenant appui sur la technique AMDEC. Elle permet de déterminer les exigences de maintenance préventive applicables et efficaces liées aux équipements, en fonction des conséquences des défaillances identifiables et du mécanisme de dégradation responsable de ces défaillances.
B 23	Analyse des conditions insidieuses (analyse transitoire)		HAZOP (B-06) AMDE (B-13) Arbre de panne (B-14)	L'analyse transitoire est une méthodologie permettant de reconnaître les erreurs de conception susceptible de causer un événement indésirable ou de gêner l'occurrence d'un événement souhaité. Cette technique a été développée dans le domaine informatique. Dans le cadre de l'examen d'un même système plusieurs outils peuvent être utilisés, tels que des arbres de panne, l'analyse des modes de défaillance et de leurs effets - AMDE (B-13) ou d'autres types d'analyse de type HAZOP. Leur combinaison permet de construire un réseau arborescent, d'évaluer les chemins de réseau et de produire des recommandations correctives.

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 24	Analyse de Markov	Σ		Cette méthode s'applique à la modélisation des facteurs contribuant à la sureté de fonctionnement de systèmes techniques (panne, réparation, modification, configuration…). Elle est généralement utilisée pour analyse des systèmes réparables comportant plusieurs états (complètement opérationnel, partiellement opérationnel, défaillant). La vitesse de passage d'un état à l'autre est représentée par une probabilité de changement pour des événement ponctuels (ou « discrets ») ou par un taux de défaillance et/ou la fréquence de réparation pour des événements continus.
B 25	Simulation de Monte-Carlo	Σ		Il s'agit d'un modèle algorithmique permettant d'évaluer les effets de l'incertitude sur les systèmes dans un large éventuel de situations. Des simulations sont établies sur la base de variables aléatoires (entrées) pour générer différents résultats de sortie ; les valeurs sélectionnées pour les entrées sont issues de distributions de probabilités appropriées représentant le degré d'incertitude pour ces paramètres. Cette technique est par exemple pertinente pour une démarche de réduction des risques associés à des décisions financières.
B 26	Analyse bayesienne et réseaux de Bayes	Σ	Modèle de Monte-Carlo (B-25)	Cette méthode repose sur le postulat que toute information déjà connue peut être combinée à une mesure subséquente afin d'établir une probabilité globale. Les entrées sont analogues à celles du modèle de Monte-Carlo; toutefois les statistiques bayésiennes se distinguent des statistiques classiques en ce sens qu'elles ne supposent pas que tous les paramètres de distribution sont fixes mais qu'il s'agit de variables aléatoires (subjectives). …/…

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
	Analyse bayesienne et réseaux de Bayes (suite)			Les réseaux de Bayles utilisent un modèle graphique pour représenter un ensemble de variables et leurs relations de probabilité, ce réseau est composé de nœuds représentant une variable aléatoire et de flèches reliant un nœud parent à un nœud enfant (un nœud parent a un effet direct sur un nœud enfant).
B 27	Courbes FN		Modèle ALARP (Annexe 3)	Il s'agit d'une représentation graphique de la probabilité de tous les événements à l'origine d'un niveau donné de nuisance dont fait l'objet une population déterminée. Les courbes FN illustrent ainsi la fréquence cumulée (F) à laquelle au moins N membres de la population seront affectés ; La valeur donnée à N rend compte notamment du degré d'acceptabilité social et politique de l'événement / du risque étudié. Cette représentation est généralement associée à l'évaluation d'un nombre de pertes et se rapproche du modèle ALARP (voir en Annexe 3).
B 28	Indices de risque	Σ	Arbre de panne (B-14) Arbre d'événement (B-15)	Cette méthode peut être utilisée pour le classement des différents risques associés à une activité lorsque le système est bien compris et documenté. Les risques sont classés à l'aide de critères analogues dans le but de les comparer ; chaque composante du risque est analysée/pointée au regard de ses sources, de l'étendue des vecteurs d'exposition possibles et des éléments susceptibles d'être affectés. Il est possible d'utiliser des outils comme l'arbre d'analyse de panne, l'analyse par arbre d'événement et l'analyse de décision générale pour appuyer le développement des indices de risque. Dans la mesure du possible, les composantes du risque et les facteurs aggravants font l'objet d'une évaluation quantitative ; le développement d'un indice est une démarche itérative, plusieurs combinaisons de pointages pouvant être testées avant que l'analyse ne maîtrise la validation.

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 29	Matrice conséquences/ probabilité		HAZOP (B-06) AMDEC (B-13)	Il s'agit ici de combiner des classements qualitatifs ou semi-quantitatifs de conséquence et de probabilité pour générer un niveau de risque ou un classement des risques. Pour un processus déterminé, une matrice est établie avec deux entrées correspondant à la conséquence et à la probabilité ; elle est généralement utilisée comme outil de dépistage lorsque de nombreux risques sont identifiés afin d'identifier ceux qui doivent faire l'objet d'une analyse plus détaillée, ceux qui doivent être traités en priorité et ceux qui peuvent être considérés comme acceptables. La matrice conséquence-probabilité peut également être utilisée pour faciliter une compréhension partagée des niveaux qualitatifs des risques à l'échelle d'une organisation. Cet outil permet également de soutenir l'examen critique d'une analyse AMDEC ou de définir des priorités à la suite d'une analyse HAZOP ; il constitue en outre une option pertinente lorsque les données d'analyse détaillée ne sont pas suffisantes ou si les conditions ne sont pas réunies pour une analyse plus quantitative. Des échelles de classement quantitatives peuvent néanmoins être utilisées, par exemple dans un contexte de fiabilité, l'échelle de probabilité pourrait représenter des taux de défaillance indicatifs et l'échelle de conséquence le coût en valeur numéraire de la défaillance (par fourchette de coût). Des échelles de 3, 4 ou 5 points sont les plus usuelles ; les échelles de conséquence et de probabilité peuvent être différentes. Pour classer les risques, il convient d'abord de décrire les conséquences correspondant le mieux à la situation puis de définir la probabilité d'occurrence de ces conséquences. .../...

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
	Matrice conséquences/ probabilité (suite)			La probabilité la plus faible doit être acceptable pour la conséquence définie comme étant la plus élevée, sinon toutes les activités aux conséquences les plus élevées seraient définies comme intolérables. Les niveaux de risque peuvent être liés aux règles de décision, comme le niveau donné à l'attention de gestion ou l'échelle de temps pour la mise en œuvre d'une réponse appropriée.
B 30	Analyse coût/bénéfice		Modèle ALARP (Annexe 3)	Cette méthode d'analyse peut être utilisée pour évaluer les risques lorsque les coûts prévus sont pondérés en fonction d'avantages attendus afin de choisir l'option la plus avantageuse. Elle peut être qualitative, quantitative ou reposer sur une combinaison de ces deux éléments. Dans l'approche quantitative, la valeur pécuniaire de tous les coûts et bénéfices afférents à un domaine d'application donné est d'abord agrégée puis ajustée au regard des durées pendant lesquelles les coûts et bénéfices considérés sont actifs. Tous les coûts et bénéfices sont exprimés en valeur actualisée vis-à-vis de l'ensemble des parties prenantes. Leur combinaison permet d'obtenir une valeur actualisée nette (VAN) qui est une entrée pour les décisions relatives au risque. Une VAN positive associée à une action indique en général qu'il convient d'entreprendre cette action ; cependant pour les risques les plus critiques engageant des vies humaines ou des questions environnementales importantes, le principe ALARP peut être appliqué - voir Annexe 3. L'exercice aboutit généralement à un tableau de comparaison des coûts et bénéfices de différents types pour chaque option étudiée. Ces éléments dessinent différents compromis qui sont proposés à l'appréciation des instances dirigeantes de l'organisation.

	Désignation	Catégorie	Outils & méthodes associés	Descriptif
B 31	Analyse de décision à critères multiples (ADCM)			Il s'agit d'une méthode d'analyse permettant d'évaluer de manière objective et transparente la valeur globale d'un ensemble d'options en réponse à un ou plusieurs objectif(s) défini(s). L'analyse repose sur l'élaboration d'une matrice d'options et de cratères qui sont classés et agrégés en vue de documenter un choix. Un groupe d'experts est chargé de déterminer les attributs attachés à chaque objectif (critères ou mesures de performance) ; il lui revient ensuite de formaliser les options à évaluer en fonction de ces critères. L'étape suivante consiste à déterminer l'importance des critères et à attribuer des facteurs de pondération correspondants. Enfin, le groupe d'experts évalue les alternatives par rapport aux critères, par exemple sous la forme d'une matrice de pointage (tableau détaillant les notes données à chaque option à raison des critères retenus) et fournit une agrégation des résultats obtenus. Cet exercice de revue permet d'établir un classement ordonné préférentiel des options disponibles.

> Documents de référence

Méthode HAZOP - B-6

- CEI 61882 - Etudes de danger et d'exploitabilité (Etudes HAZOP) - Guide d'application

Analyse des dangers - Points critiques pour leur maîtrise (HACCP) - B-7

- ISO 22000 - Systèmes de management de la sécurité des denrées alimentaires - Exigences pour tout organisme appartenant à la chaîne alimentaire

Analyse des modes de défaillance et de leurs effets (AMDE) - Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) - B-13

- CEI 60812 - Techniques d'analyse de la fiabilité du système - Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)

Analyse par arbre de panne - B-14

- CEI 61025 - Analyse par arbre de panne (APP)
- CEI 60300-3-9 - Gestion de la sécurité de fonctionnement - Partie 3 : Guide d'application - Section 9 : Analyse du risque des systèmes technologiques

Layer of Protection Analysis - LOPA - B-18

- CEI 61508 (toutes les parties) - Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
- CEI 61511 - Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation

Analyse de Markov - B-24

- CEI 61078 - Techniques d'analyse pour la sûreté de fonctionnement - Bloc-diagramme de fiabilité et méthodes booléennes
- CEI 61165 - Application des techniques de Markov
- ISO/IEC 15909 (toutes les parties) - Systems and software engineering - High-level Petri nets

Simulation de Monte-Carlo - B-25

- CEI 61649 - Analyse de Weibull
- CEI 62551 - Techniques d'analyse pour la sûreté de fonctionnement - Modélisation par réseau de Pétri
- Guide ISO/CEI 98-3 :2008 - Uncertainty measurement - Part 3 : Guide to the of uncertainty in measurement (GUM :1995)

Fiche technique 11 > Annexe 1

Techniques de brainstorming

Le brainstorming peut être utilisé tout au long du processus d'évaluation des risques.

I. Objectifs

Le brainstorming vise à stimuler la capacité à faire émerger collectivement des réponses originales et pertinentes en réponse à un problème posé, tant au regard des solutions recherchées que de l'analyse des causes.

Selon les nécessités, cet exercice peut utiliser comme support un Diagramme Cause/Effet ou prendre appui sur un Schéma heuristique présentant l'ensemble des aspects et enjeux de la question étudiée.

II. Méthode

Une séance de brainstorming se pratique en groupe et doit être contenue dans un temps court (d'une à deux heures) afin de maintenir un rythme soutenu d'échanges et de rebonds entre participants.

Cette démarche s'applique aux différentes étapes d'une démarche de résolution de problème : analyser les risques, rechercher les causes possibles d'un dysfonctionnement, rechercher des mesures correctives…

Pour réunir les meilleures chances de succès il convient d'organiser le brainstorming en quatre étapes successives, d'assigner à chacune d'entre elles un objectif particulier et de la contenir dans un laps de temps limité.

La conduite de la réunion est confiée à un animateur spécifiquement désigné qui sera en charge des diverses tâches associées à chaque étape.

Celui-ci veille à ce que la salle où se tient le brainstorming est équipée d'un tableau et dispose de tout le matériel nécessaire à la prise rapide de notes.

Etapes d'un exercice de brainstorming

Etape	Tâches associées (à la charge de l'animateur du groupe)	Durée
Lancement de la réunion	▪ Ecrire et afficher le problème qui fait l'objet du brainstorming ▪ Ecrire et afficher les règles comportementales dont dépend le succès de l'exercice[157]	5 à 10 minutes
Discussion des idées primaires	▪ Solliciter un large échange de vues sur les différents aspects et enjeux du problème posé ▪ Noter au tableau toutes les idées émises ▪ Veiller à ce que tous les participants s'expriment ▪ Recentrer le groupe s'il s'éloigne trop du problème de départ en reformulant celui-ci. ▪ Soutenir le rythme d'émission d'idées en relançant en permanence à partir des différents aspects du problème et en stimulant les associations d'idées par des verbes-clés ▪ Si le choix a été fait d'utiliser un schéma heuristique (map minding) celui-ci peut être rempli et complété dès cette étape	5 à 30 minutes
Approfondissement des idées primaires	▪ Proposer une rapide synthèse pour dégager les idées à approfondir en prenant soin de ne fermer aucun champ d'investigation ▪ Approfondir les idées sélectionnées en sollicitant un nouvel échange de vues en donnant plus de temps à chaque intervenant pour exposer sa position ▪ Reformuler les idées jusqu'à ce qu'elles soient compréhensibles en dehors du groupe ▪ Ecarter toute opinion subjective ou tout jugement de valeur sur les idées énoncées	1 heure maximum
Exploitation des idées produites	▪ Valider ou rejeter en séance par consensus chacune des idées produites ▪ Formaliser les idées validées sur un support approprié à l'objectif initial du brainstorming (diagramme cause / effet, tableau d'actions correctives…)	5 à 30 minutes

[157] Ces règles sont : ne pas critiquer, ne pas s'autocensurer, émettre des idées à partir des idées des autres, s'exprimer brièvement

Fiche technique 11 > Annexe 2

Diagramme Cause/Effet ou diagramme d'Ishikawa

Cette représentation graphique permet d'identifier l'ensemble des causes d'un dysfonctionnement constaté.

Il prend la forme d'une arborescence construite sur le dysfonctionnement constaté et déployée jusqu'à faire apparaître toutes ses causes possibles, soit les causes principales (branches), les causes secondaires (petites branches) et les détails (feuilles).

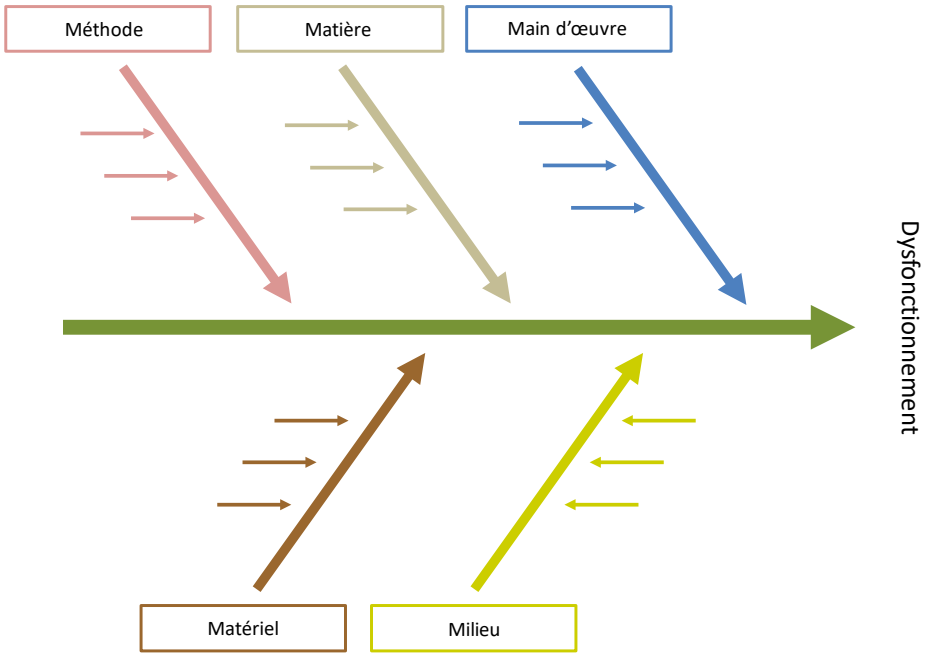
Cet ordonnancement permet de visualiser simplement le poids relatif de chaque cause et de déterminer ainsi les causes sur lesquelles il convient d'agir en priorité.

Les causes possibles du dysfonctionnement se répartissent entre cinq familles (ou 5 M).

Causes possibles du dysfonctionnement	Exemples
Main d'œuvre	Poste vacant, personnel non suffisamment formé ou insuffisant pour les tâches à réaliser…
Matière	Défaut d'approvisionnement, indisponibilité des fournitures requises…
Méthode	Complexité du circuit de traitement, périodicité inadaptée…
Matériel	Outil informatique obsolète, défaillant ou inapproprié…
Milieu	Eloignement géographique des acteurs…

Méthode

Le Diagramme Cause/Effet est établi à partir du canevas suivant.



Sur cette base et dans le cadre d'un échange collectif il est procédé à un recensement de l'ensemble des causes possibles du dysfonctionnement constaté.

La recherche de ces causes prend appui sur l'ensemble de la documentation collectée ainsi que sur les conclusions des Observations éventuellement réalisées sur place.

Ces causes sont classées par famille et par ordre d'importance (des causes prépondérantes jusqu'aux causes secondaires) puis sont positionnées en conséquence dans le diagramme.

En cas de besoin, deux causes additionnelles peuvent être ajoutées :

- Management,
- Moyens financiers.

Lorsque le diagramme est renseigné, il est utile de vérifier sur place que les causes retenues engendrent effectivement l'effet observé ; à défaut le groupe de travail doit être de nouveau réuni pour revoir et corriger le diagramme.

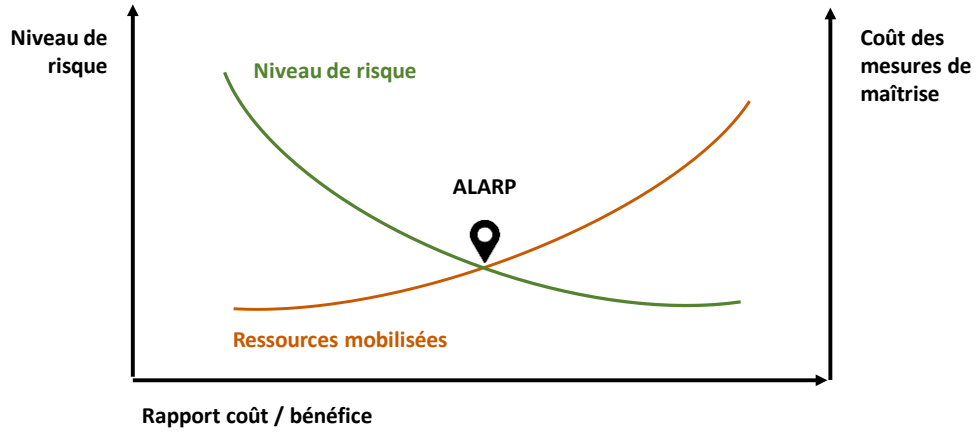
Fiche technique 11 > Annexe 3

Visualisation de l'arbitrage coût/avantage d'une maîtrise des risques - Méthode ALARP (As low as reasonably practicable)

D'abord développé au titre de la prévention de la prévention des accidents industriels et environnementaux majeurs, le concept de ALARP représente le point d'aboutissement d'une démarche de management des risques intégrant une double approche de sécurisation des activités de l'organisation et d'optimisation des moyens de maîtrise dédiés.

Cet acronyme désigne ainsi un niveau de risque tolérable ou qui ne peut être réduit sans exposer l'organisation à des coûts excédant les avantages attendus ou encore hors de portée technique et/ou logistique.

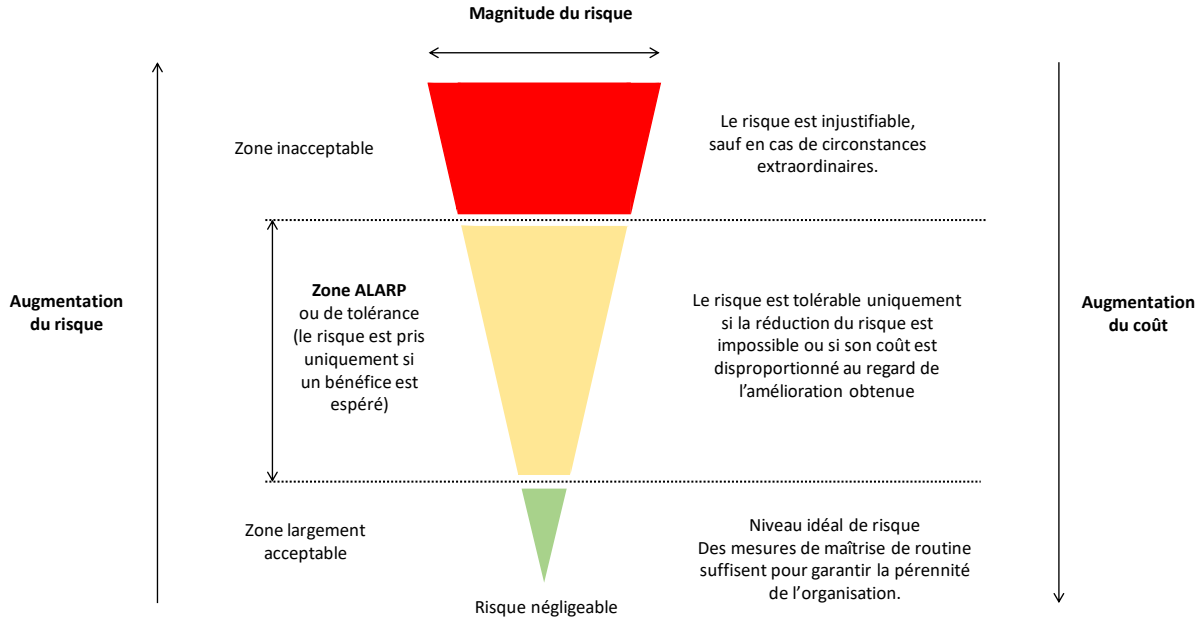
Pour chaque risque étudié, il s'agit de déterminer un point d'équilibre entre le degré d'exposition résiduel de l'organisation et le coût des mesures de maîtrise afférentes.



La mesure de ces valeurs requiert quelques précautions méthodologiques :

- l'appréciation du niveau de risque doit prendre appui sur un historique de données couvrant une durée significative (au moins deux années échues en principe) à moins de disposer d'autres outils d'évaluation offrant au moins les mêmes garanties (données fiables, disponibles et statistiquement représentatives) :
- il importe d'intégrer l'ensemble des coûts de maîtrise directs ou indirects afférents au risque étudié.

De manière générale, l'utilisation de la méthode ALARP est pertinente pour l'examen de certains risques critiques engageant la continuité des activités de l'organisation ; ces risques extrêmes doivent être contenus hors le cas de leur coût disproportionné ou de difficultés matérielles et/ou techniques insurmontables.



Fiche technique 12

Exemples d'échelles de criticité des risques

La criticité d'un risque est une combinaison de son impact et de sa probabilité.

Ces deux facteurs sont mesurés séparément, en utilisant des échelles distinctes ; il peut toutefois être avantageux d'utiliser la même graduation afin de pouvoir aisément établir une valeur synthétique unique qui pourra être rapprochée du degré de maîtrise du même risque[158].

I. Mise en place d'une échelle d'impact

Différentes échelles peuvent être proposées pour déterminer l'impact d'un risque.

Dans l'exemple suivant, une échelle de 1 à 5 décrit la progression des conséquences de la survenance d'un risque sur le fonctionnement de la collectivité.

Classe de gravité	Intitulé de la classe	Intitulé des conséquences
1	Mineure	Aucun impact sur les performances et la sécurité de l'activité
2	Significative	Dégradation des performances du système sans impact sur la sécurité
3	Grave	Forte dégradation ou échec des performances du système sans impact sur la sécurité
4	Critique	Dégradation de la sécurité ou de l'intégrité du système
5	Catastrophique	Forte dégradation ou échec de la sécurité ou perte du système

Si le besoin s'en fait sentir, la gravité de l'impact peut être plus finement mesurée au regard de divers types de conséquences ; le choix des conséquences à examiner dépend de la nature du risque examiné et peut donc évoluer selon les cas.

Classe de gravité et intitulé	Note de 1 à 5 Conséquences sur les biens matériels et immatériels	Note de 1 à 5 Conséquences sur les personnes	Note de 1 à 5 Conséquences sur l'environnement	Note de 1 à 5 Conséquences sur les performances	Note de 1 à 5 Etc…
1 – Mineure					
2 – Significative					
3 – Grave					
4 – Critique					
5- Catastrophique					

[158] Voir Fiche technique n° 13

Dans l'**exemple** ci-après, la gravité d'un événement est mesurée au regard des critères suivants :

1. Impact sur la conduite de la mission ;
2. Impact sur le respect des délais ;
3. Impact sur la sécurité des personnes ;
4. Impact sur la sécurité des données.

Il peut être décidé que le degré de gravité (entre 1 et 5) attribué à l'événement correspond au degré de gravité le plus élevé enregistré sur ces quatre critères ; de manière alternative le degré de gravité de l'événement peut être établi sur base d'une note moyenne pour les quatre critères ou correspondre à la note atteinte pour le plus grand nombre de critères.

Gravité	Critères	Intitulé des conséquences
Classe 1 Mineure	Générique	Aucun impact sur les performances et la sécurité de l'activité
	1 - Mission	Système en situation de poursuivre la mission en mode nominal
	2 - Délais	Aucun retard enregistré
	3 - Personnes	Pas de victime
	4 - Données	Aucune compromission de données
Classe 2 Significative	Générique	Dégradation des performances du système sans impact significatif en matière de sécurité
	1 - Mission	Le système peut continuer la mission en mode légèrement dégradé
	2 - Délais	Faibles retards sans impact sur le déroulement de la mission
	3 - Personnes	Nombre très réduit d'accidents corporels
	4 - Données	Compromission de données sensibles mais non confidentielles
Classe 3 Grave	Générique	Forte dégradation ou mise en échec des performances du système avec un impact réduit sur la sécurité
	1 - Mission	Système en situation de poursuivre la mission en mode dégradé
	2 - Délais	Retards de nature à perturber le déroulement de la mission
	3 - Personnes	Nombre significatif d'accidents corporels
	4 - Données	Compromission de données confidentielles
Classe 4 Critique	Générique	Dégradation de la sécurité ou de l'intégrité du système
	1 - Mission	Système en situation de poursuivre la mission en mode très dégradé
	2 - Délais	Retards de nature remettre en cause le déroulement de la mission
	3 - Personnes	Nombre important d'accidents corporel, y compris invalidants
	4 - Données	Compromission de données cruciales
Classe 5 Catastrophique	Générique	Forte dégradation ou échec de la sécurité ou perte du système
	1 - Mission	Système impropre à la poursuite de la mission
	2 - Délais	Retards propres à entraîner un échec ou un abandon de la mission
	3 - Personnes	Accidents corporels graves, décès éventuels
	4 - Données	Compromission de données tenues secrètes

Exemple de grille d'impact des risques : suites données à la communication d'informations préoccupantes dans le domaine de la protection de l'enfance

Classe	Cible d'impact	Description des conséquences
1 **Mineure** **Aucun impact**	Générique	Aucun impact sur les performances et la sécurité de l'activité
	Agent	Gêne ou mécontentement d'un agent
	Usager	Gêne ou mécontentement d'un usager
	Image	Aucun impact sur l'image du Département
	Juridique	Aucun impact juridique
	Organisation	Aucun impact sur l'organisation
2 **Significative** **Mission dégradée**	Générique	Dégradation des performances du système sans impact sur la sécurité
	Agent	Difficultés dans l'exercice de ses missions peu impactant ou situation surmontable sans difficultés pour l'agent
	Usager	Réclamation verbale ou écrite d'un usager
	Image	Image du Département affectée uniquement en interne
	Juridique	Demande d'éclairage interne hiérarchique
	Organisation	Surcharge de travail temporaire et compensable
3 **Grave** **Mission échouée**	Générique	Forte dégradation ou échec des performances du système sans impact sur la sécurité
	Agent	Difficultés dans l'exercice de ses missions impactant ou situation surmontable avec difficultés par l'agent
	Usager	Mise en difficulté financière modérée, retard de prise en charge peu impactant ou situation surmontable sans difficultés par l'usager
	Image	Image de la collectivité affectée à l'extérieur pendant un bref délai (média alternatif, réseaux sociaux, associations d'usagers, intervention d'élus, ...)
	Juridique	Contentieux sans contrepartie financière
	Organisation	Surcharge de travail durable et compensable
4 **Critique** **Sécurité dégradée**	Générique	Dégradation de la sécurité ou de l'intégrité du système
	Agent	Situation de stress et de mal-être au travail (RPS) pour l'agent sans arrêt de travail
	Usager	Mise en difficulté financière importante, retard de prise en charge impactant ou situation surmontable avec difficultés pour l'usager
	Image	Image de la collectivité affectée à l'extérieur à moyen terme (presse locale/régionale)
	Juridique	Contentieux avec contrepartie financière
	Organisation	Surcharge de travail durable et non compensable
5 **Catastrophique** **Sécurité échouée**	Générique	Forte dégradation ou échec de la sécurité ou perte du système
	Agent	Situation de stress et de mal-être au travail (RPS) pour l'agent avec arrêt de travail
	Usager	Mise en danger ou situation insurmontable pour l'usager
	Image	Image de la collectivité affectée à l'extérieur à long terme (presse nationale)
	Juridique	Condamnation pénale de la collectivité et/ou d'un agent
	Organisation	Blocage de l'organisation

Exemple de grille d'impact des risques : pilotage de la prestation de compensation de handicap

Classe	Cible d'impact	Description des conséquences
1 Mineure Aucun impact	Générique	Aucun impact sur les performances et la sécurité de l'activité
	Agent	Gêne ou mécontentement d'un agent
	Usager	Gêne ou mécontentement potentiel d'un usager
	Image	Aucun impact sur l'image du Département et/ou de la MDPH
	Juridique	Conciliation (demande d'éclairage)
	Organisation	Aucun impact sur l'organisation
	Financier	Aucun impact financier
2 Significative Mission dégradée	Générique	Dégradation des performances du système sans impact sur la sécurité
	Agent	Difficultés dans l'exercice de ses missions peu impactant ou situation surmontable sans difficultés pour l'agent
	Usager	Réclamation verbale ou écrite d'un usager
	Image	Image de la collectivité affectée uniquement en interne
	Juridique	Recours administratif préalable obligatoire (réexamen du dossier sous 2 mois)
	Organisation	Surcharge de travail temporaire et compensable
	Financier	Génération d'indus
3 Grave Mission échouée	Générique	Forte dégradation ou échec des performances du système sans impact sur la sécurité
	Agent	Difficultés dans l'exercice de ses missions impactant ou situation surmontable avec difficultés par l'agent
	Usager	Mise en difficulté financière modérée, retard de prise en charge peu impactant ou situation surmontable sans difficultés par l'usager
	Image	Image de la collectivité affectée à l'extérieur pendant un bref délai (média alternatif, réseaux sociaux, associations d'usagers, intervention d'élus, baisse de l'indicateur de satisfaction générale, ...)
	Juridique	Contentieux (modification de la décision) sans dommages et intérêts
	Organisation	Surcharge de travail durable et compensable
	Financier	Non récupération d'indus
4 Critique Sécurité dégradée	Générique	Dégradation de la sécurité ou de l'intégrité du système
	Agent	Situation de stress et de mal-être au travail (RPS) pour l'agent sans arrêt de travail
	Usager	Mise en difficulté financière importante, retard de prise en charge impactant ou situation surmontable avec difficultés par l'usager
	Image	Image de la collectivité affectée à l'extérieur à moyen terme (presse locale)
	Juridique	Contentieux (modification de la décision) avec dommages et intérêts
	Organisation	Surcharge de travail durable et non compensable
	Financier	Dépenses supplémentaires ne pouvant pas faire l'objet de virement au sein de la même sous-fonction
5 Catastrophique Sécurité échouée	Générique	Forte dégradation ou échec de la sécurité ou perte du système
	Agent	Situation de stress et de mal-être au travail (RPS) pour l'agent avec arrêt de travail
	Usager	Mise en danger ou situation insurmontable par l'usager
	Image	Image de la collectivité affectée à l'extérieur à long terme (presse nationale)
	Juridique	Condamnation pénale de la collectivité et/ou de la MDPH et/ou d'un agent
	Organisation	Blocage de l'organisation
	Financier	Dépenses supplémentaires ne pouvant pas faire l'objet de virement

Exemple de grille d'impact des risques : sécurisation du processus de délégation de signature

Classe	Cible d'impact	Description des conséquences
1 Mineure Aucun impact	Générique	Aucun impact sur les performances et la sécurité de l'activité
	Agent	Gêne ou mécontentement d'un agent
	Usager	Gêne ou mécontentement d'un usager
	Image	Aucun impact sur l'image du Département
	Juridique	Aucun impact juridique
	Organisation	Aucun impact sur l'organisation
2 Significative Mission dégradée	Générique	Dégradation des performances du système sans impact sur la sécurité
	Agent	Difficultés dans l'exercice de ses missions peu impactant ou situation surmontable sans difficultés pour l'agent
	Usager	Réclamation verbale ou écrite d'un usager
	Image	Image de la collectivité affectée uniquement en interne
	Juridique	Demande d'éclairage interne hiérarchique
	Organisation	Surcharge de travail temporaire et compensable
3 Grave Mission échouée	Générique	Forte dégradation ou échec des performances du système sans impact sur la sécurité
	Agent	Difficultés dans l'exercice de ses missions impactant ou situation surmontable avec difficultés par l'agent
	Usager	Mise en difficulté financière modérée, retard de prise en charge peu impactant ou situation surmontable sans difficultés par l'usager
	Image	Image de la collectivité affectée à l'extérieur pendant un bref délai (média alternatif, réseaux sociaux, associations d'usagers, intervention d'élus, ...)
	Juridique	Contentieux sans contrepartie financière
	Organisation	Surcharge de travail durable et compensable
4 Critique Sécurité dégradée	Générique	Dégradation de la sécurité ou de l'intégrité du système
	Agent	Situation de stress et de mal-être au travail (RPS) pour l'agent sans arrêt de travail
	Usager	Mise en difficulté financière importante, retard de prise en charge impactant ou situation surmontable avec difficultés pour l'usager
	Image	Image de la collectivité affectée à l'extérieur à moyen terme (presse locale/régionale)
	Juridique	Contentieux avec contrepartie financière
	Organisation	Surcharge de travail durable et non compensable
5 Catastrophique Sécurité échouée	Générique	Forte dégradation ou échec de la sécurité ou perte du système
	Agent	Situation de stress et de mal-être au travail (RPS) pour l'agent avec arrêt de travail
	Usager	Mise en danger ou situation insurmontable pour l'usager
	Image	Image de la collectivité affectée à l'extérieur à long terme (presse nationale)
	Juridique	Condamnation pénale de la collectivité et/ou d'un agent
	Organisation	Blocage de l'organisation

II. Mise en place d'une échelle de probabilité / de fréquence

La fréquence d'un risque est appréciée au regard de son impact.

Dans l'exemple suivant, une échelle de 1 à 5 décrit la répétition attendue d'un événement sur des périodes de temps croissantes.

Niveau de fréquence	Intitulés	Survenance de l'événement	Période de retour
F1	Impossible à improbable	Moins d'une fois par T1	
T1			5 ans
F2	Très peu probable	Entre une fois par T1 une fois par T2	
T2			1 an
F3	Peu probable	Entre une fois par T2 une fois par T3	
T3			1 mois
F4	Probable	Entre une fois par T3 une fois par T4	
T4			1 semaine
F5	Très probable à certain	Plus d'une fois par T4	

Le degré de fréquence attribué à un événement peut être vérifié *in itinere* et éventuellement corrigé.

A cet effet, la collectivité pourra mettre en place un Journal de bord permettant d'enregistrer et dater chaque épisode nouveau ; la tenue sur la durée d'un tel journal permet d'optimiser la traçabilité de la valeur attribuée.

Fiche technique 13

Proposition pour la mise en place d'une échelle de maîtrise des risques

---

L'échelle de maîtrise des risques se comprend en premier lieu au regard de l'efficience des dispositifs de contrôle interne y afférents et permet de mesurer l'écart entre les systèmes effectifs observés et une situation optimale caractérisée par :

- une connaissance précise et parfaitement actualisée des risques auxquels est exposée la collectivité ;
- des contrôles et tests pleinement intégrés aux pratiques métier, exécutés sans erreur et à l'échéance souhaitée ;
- la mise en œuvre actions ciblées pour améliorer de manière continue la maîtrise des processus concernés.

L'échelle de maîtrise des risques vise à mettre tout responsable de dispositif en situation *« de comparer sa démarche de contrôle interne par rapport à ce schéma cible et d'évaluer sa maturité* »[159], le cas échéant en procédant par palier.

Pour évaluer le degré de maîtrise des risques identifiés, une collectivité peut recourir à l'échelle de notation présente dans le référentiel COSO 2013 dédié au contrôle interne.

Le cheminement proposé dans ce cadre prend la forme de 5 niveaux successifs ; il trouve son point de départ avec un environnement imprévisible où il n'y a ni organisation maîtrisée ni procédures, puis progresse à mesure qu'un dispositif de contrôle interne efficace se met en place et que le système acquiert des mécanismes adéquats de correction des dysfonctionnements constatés.

Une approche similaire par degré de maturité se retrouve dans d'autres méthodes et techniques d'analyse fonctionnelle comme le référentiel COBIT 5, qui est particulièrement en usage pour le pilotage des Systèmes d'information.

Le référentiel CobiT 5 propose un modèle de maturité pour chaque processus afin de le situer par rapport aux meilleures pratiques du marché.

Ce modèle comprend 6 niveaux numérotés 0 à 5.

Chacun des échelons successifs correspond à un niveau plus élaboré et plus efficient de gouvernance des systèmes d'information d'une organisation.

Le degré d'efficience obtenu se mesure notamment en termes d'auditabilité et de prédictibilité.

Une collectivité peut trouver avantage à fusionner les grilles issues des référentiels COSO 2013 et COBIT 5 pour établir une seule échelle de notation couvrant l'ensemble des critères d'appréciation pertinents.

---

[159] DGFiP. (2010). *Echelle de maturité de la gestion des risques.* https://www.economie.gouv.fr/files/modop_echelle.pdf

Proposition d'échelle de maîtrise des risques

	Descriptif (Contrôle Interne)	Correspondance COBIT 5
Degré 5 **Optimisé**	On observe une conformité totale à l'énoncé des éléments attendus, en principe et en pratique, à tout moment et partout. Le dispositif fait l'objet d'une supervision globale et régulière. Un référentiel intégré de contrôle interne est surveillé en temps réel par le management et en amélioration continue. Des outils - automatisés ou non - sont utilisés de manière avancée pour supporter des activités de contrôles et permettre à la collectivité d'améliorer en continu les activités considérées.	**Processus en optimisation** Le processus prévisible décrit précédemment est amélioré continuellement afin d'atteindre les objectifs d'affaires pertinents actuels et projetés
Degré 4 + **Supervisé +**	Le management souscrit totalement au principe, mais, en pratique, la conformité n'est encore que partielle. Les contrôles sont standardisés et périodiquement testés pour s'assurer de l'efficacité de leur conception et de leur application. Ils font l'objet d'un reporting au management. Des outils automatisés ou non peuvent être utilisés pour supporter des activités de contrôles.	**Processus prévisible** Le processus établi décrit précédemment fonctionne maintenant selon des limites définies qui assurent l'atteinte des résultats souhaités
Degré 4 **Supervisé**		**Processus établi** Le processus géré décrit précédemment est maintenant mis en œuvre selon une procédure définie qui permet l'atteinte des résultats souhaités
Degré 3 **Standardisé**	Les contrôles existent et sont appliqués ; ils sont documentés et diffusés aux collaborateurs. Il y a lieu d'observer une conformité limitée à l'énoncé des éléments attendus ainsi qu'une adhésion au principe mais non accompagnée de l'ensemble des effets désirés. Des déviations non détectées peuvent apparaître.	**Processus géré** Le processus exécuté décrit précédemment est maintenant mis en œuvre et bien géré (planifié, surveillé et ajusté), et ses résultats sont adéquatement établis, contrôlés et maintenus.

Proposition d'échelle de maîtrise des risques (suite)

	Descriptif (Contrôle Interne)	Correspondance COBIT 5
Degré 2 **Informel**	Une conformité limitée avec les exigences requises. Le management soutient le principe d'un management des risques, mais en pratique, l'application des règles est médiocre. Il existe des pratiques de contrôle mais elles sont insuffisamment documentées et reposent sur des interventions ponctuelles à l'initiative des agents concernés. Les contrôles reposent ainsi essentiellement sur des individus ; il n'y a pas de formations formelles ou de communication sur les activités de contrôles.	**Processus exécuté** Le processus mis en œuvre réalise la fonction désirée.
Degré 1 **Non fiable**	Très peu voire pas de conformité avec les exigences requises. Environnement non prédictible sur lequel des contrôles n'ont pas été définis et/ou ne sont pas appliquées.	**Processus incomplet** Le processus n'est pas mis en œuvre ou ne parvient pas à réaliser la fonction désirée. À ce niveau, il y a peu de preuves, voire aucune, que l'objectif du processus est atteint systématiquement.

Fiche technique 14

Normes professionnelles de l'audit interne

La dernière version du Cadre de référence international des pratiques professionnelles (CRIPP) de l'audit interne a été publiée en 2017.

Les activités d'audit interne présentées ci-après répondent à la définition qui en est donnée dans le CRIPP :

> « *L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance, et en faisant des propositions pour renforcer leur efficacité*. »

Le CRIPP est approuvé par l'IIA (*Institute of Internal Auditors*) dont l'objet est d'établir et actualiser les standards professionnels d'audit interne à l'échelle internationale.

Le CRIPP contient les éléments suivants :

- un énoncé de Principes fondamentaux pour la pratique professionnelle de l'audit interne ;
- un **Code de Déontologie** contenant les principes d'éthique attendus au sein de la profession d'audit interne ;
- un corpus des normes applicables aux missions d'audit interne ;
- un Glossaire des principaux termes utilisés ;
- un ensemble de Lignes directrices de mise en œuvre visant à expliciter le cadre opérationnel des normes applicables.

Les normes applicables se répartissent en deux catégories distinctes :

- Les normes de qualification (Norme 1000 à Norme 1322) énoncent les caractéristiques des entités et des personnes qui réalisent des activités d'audit interne.
- Les normes de fonctionnement (Norme 2000 à Norme 2600) décrivent la nature des activités d'audit interne et définissent des critères de qualité permettant de mesurer leur performance.

Code de déontologie de l'audit interne

Le CRIPP énonce dix « Principes fondamentaux pour la pratique professionnelle de l'audit interne » qui sont le garant de la confiance placée en l'audit pour donner une assurance objective sur les processus de management des risques, de contrôle et de gouvernance.

Ces principes sont repris et développés dans un Code de Déontologie de l'IFACI qui a pour but de promouvoir une culture de l'éthique au sein de la profession d'audit interne.

Le Code de déontologie s'applique à la fois aux personnes et aux organismes qui fournissent des services d'audit interne ; il est un point d'appui évident pour les chartes d'audit des collectivités engagées dans une démarche assurantielle étendue aux trois lignes de maîtrise des risques.

L'ensemble de ces dispositions ont valeur d'obligation à l'exception des Lignes directrices de mise en œuvre qui revêtent seulement le caractère de recommandations.

Les normes doivent en particulier être observées par les auditeurs internes et à la fonction d'audit interne pour l'ensemble des missions menées.

Tous les auditeurs internes ont la responsabilité de se conformer aux normes relatives à l'objectivité, aux compétences et à la conscience professionnelle individuelles.

Ils doivent également se conformer aux normes relatives aux responsabilités associées à leur poste.

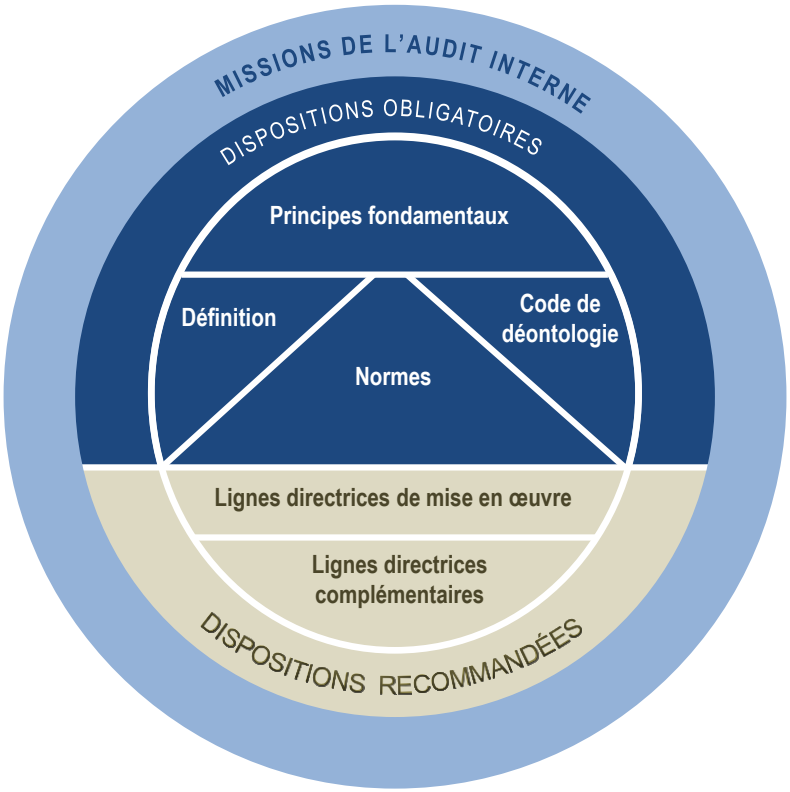
Les responsables de l'audit interne ont la responsabilité supplémentaire d'assurer la conformité globale de l'audit interne avec les normes et d'en rendre compte.

Lorsque la législation ou la réglementation empêchent la fonction d'audit interne de se conformer à certaines dispositions des normes, les dispositions non concernées restent en application et toute communication résultant de la mission en fait explicitement mention.

Si les normes sont utilisées conjointement avec des prescriptions d'autres organismes, ces dernières sont citées dans les communications de l'audit interne ; il en est ainsi notamment de la réglementation UE applicable aux programmes de la politique européenne de cohésion confiés à la Région.

Dans le cas enfin où des auditeurs internes relèveraient des divergences entre les normes et ces prescriptions ils ont la possibilité d'appliquer ces dernières si elles sont plus contraignantes.

Le schéma suivant présente le contenu du CRIPP.



Les tableaux suivants présentent la déclinaison des normes du CRIPP au sein de la collectivité régionale.

Modalités de mise en application des normes de qualification du Cadre de référence international des pratiques professionnelles (CRIPP) de l'audit interne

Les normes de qualification

Nomenclature CRIPP		
Norme 1000 - Mission, pouvoirs et responsabilités	Norme 1010	Reconnaissance des dispositions obligatoires dans la charte d'audit interne
Norme 1100 - Indépendance et objectivité	Norme 1110	Indépendance dans l'organisation
	Norme 1111	Relation directe avec le Conseil
	Norme 1112	Rôles du responsable de l'audit interne en dehors de l'audit interne
	Norme 1120	Objectivité individuelle
	Norme 1130	Atteinte à l'indépendance ou à l'objectivité
Norme 1200 - Compétence et conscience professionnelle	Norme 1210	Compétence
	Norme 1220	Conscience professionnelle
	Norme 1230	Formation professionnelle continue
Norme 1300 - Programme d'assurance et d'amélioration qualité	Norme 1310	Exigences du programme d'assurance et d'amélioration qualité
	Norme 1311	Évaluations internes
	Norme 1312	Évaluations externes
	Norme 1320	Communication relative au programme d'assurance et d'amélioration qualité
	Norme 1321	Mention de la conformité aux normes d'audit internationales
	Norme 1322	Indication de non-conformité

Modalités de mise en application des normes de fonctionnement du Cadre de référence international des pratiques professionnelles (CRIPP) de l'audit interne

Les normes de fonctionnement

Nomenclature CRIPP		
Norme 2000 - Gestion de l'audit interne	Norme 2010	Planification
	Norme 2020	Communication et approbation
	Norme 2030	Gestion des ressources
	Norme 2040	Règles et procédures
	Norme 2050	Coordination et utilisation d'autres travaux
	Norme 2060	Communication à la direction générale et au Conseil
	Norme 2070	Responsabilité de l'organisation en cas de recours à un prestataire externe pour ses activités d'audit
Norme 2100 - Nature du travail	Norme 2110	Gouvernance
	Norme 2120	Management des risques
	Norme 2130	Contrôle
Norme 2200 - Planification de la mission	Norme 2201	Considérations relatives à la planification
	Norme 2210	Objectifs de la mission
	Norme 2220	Périmètre d'intervention de la mission
	Norme 2230	Ressources affectées à la mission
	Norme 2240	Programme de travail de la mission
Norme 2300 - Réalisation de la mission	Norme 2310	Identification des informations
	Norme 2320	Analyse et évaluation
	Norme 2330	Documentation des informations
	Norme 2340	Supervision de la mission
Norme 2400 - Communication des résultats	Norme 2410	Contenu de la communication
	Norme 2420	Qualité de la communication
	Norme 2421	Erreurs et omissions
	Norme 2430	Mention de la conformité aux normes d'audit internationales
	Norme 2431	Indication de non-conformité
	Norme 2440	Diffusion des résultats
	Norme 2450	Les opinions globales
Norme 2500 - Surveillance des actions de progrès		
Norme 2600 - Communication relative à l'acceptation des risques		

Fiche technique 15

Rôle de l'audit interne dans le management des risques

I Principes généraux

La Norme 2120 du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP)[160] prévoit que l'audit interne « *doit évaluer et formuler des recommandations appropriées en vue d'améliorer les processus de gouvernance de l'organisation pour (…) la surveillance des processus de management des risques et de contrôle* ».

Cette norme est complétée des éléments d'interprétation suivants :

« *L'audit interne passe généralement en revue le processus d'évaluation annuelle des risques [et] peut également examiner les procès-verbaux de réunions au cours desquelles il a été question de stratégie de management des risques, ainsi que les évaluations des risques précédentes, s'entretenir avec les principaux responsables du management des risques tels que les responsables de la conformité, des risques et des finances. Les renseignements obtenus peuvent être comparés à des éléments de référence et aux tendances du secteur pour s'assurer que tous les risques significatifs ont bien été envisagés* ».

Il convient de noter qu'un schéma identique prévaut dans la réglementation communautaire applicable aux contrôles légaux des comptes annuels et des comptes consolidés.

La directive 2006/43/CE du Parlement européen et du conseil du 17 mai 2006 - dite également « huitième directive de l'UE relative au droit des sociétés » - dispose ainsi dans son article 41 section 2b qu'un comité d'audit institué au sein de chaque « *entité d'intérêt public* »[161] est chargé du « *suivi de l'efficacité des systèmes de contrôle interne, d'audit interne, le cas échéant, et de gestion des risques de la société* »[162].

II Eclaircissements apportés par l'IIA (*Institute of internal auditors*)

Dans un Position Paper en date de septembre 2004 (« *The role of internal auditing in Entreprise wise risk management* »)[163] l'IIA (*Institute of internal auditors*) identifie 18 tâches contribuant à la gestion des risques au sein d'organisation et les classe selon le critère de compatibilité avec les travaux d'audit, cette compatibilité étant appréciée au travers de l'indépendance de l'audit interne.

Ce document rappelle qu'il appartient à l'audit interne d'analyser le processus de management des risques dans le cadre d'une mission assurantielle portant sur les méthodes d'évaluation des risques et l'efficience du management des risques identifiés.

A l'inverse, l'audit interne ne doit pas se substituer à la direction générale de l'organisation (*top management*) en matière de prise de décision sur les niveaux de risque ni prendre directement en charge la responsabilité du management des risques car il s'exposerait ainsi à des situations de conflit d'intérêts

[160] Voir Fiche technique n° 14

[161] Au sens de l'article 2-13 de cette même directive

[162] Ces dispositions ont été intégrées dans la législation nationale suite à l'ordonnance n° 2008-1278 du 8 décembre 2008 et figurent à l'article L 823-19 du Code du Commerce.

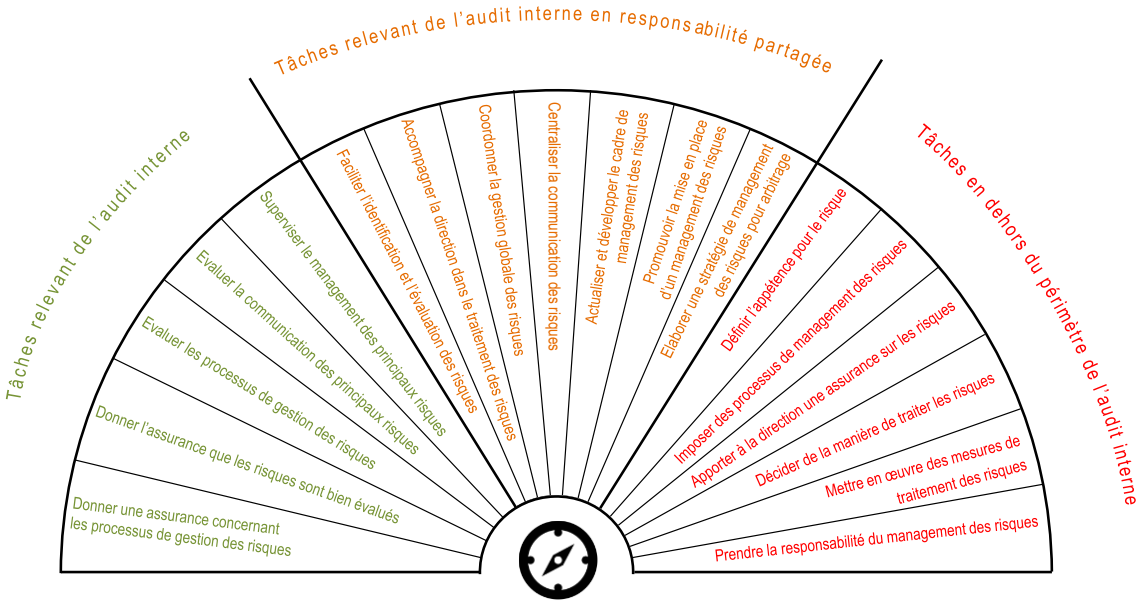
[163] La dernière mise à jour est en date de janvier 2009

lors de missions ultérieures qui seraient de nature à remettre en question l'indépendance et l'impartialité des travaux menés.

Entre ces deux postures clairement tranchées, l'audit interne peut contribuer à certains travaux de conception et d'exécution touchant en particulier l'identification et l'évaluation des risques (élaboration de la cartographie des risques) ainsi que la définition d'une stratégie globale de management des risques.

Dans ces cas de figure, l'audit interne peut assurer une fonction de conseil et/ou d'expertise, contribuer à la méthodologie de recherche et d'action - notamment en termes de communication interne et externe, de capitalisation, de benchmarking des bonnes pratiques - mais veille à n'avoir aucune part dans le processus de décision touchant l'élaboration des stratégies pertinentes.

Degrés d'implication de l'audit interne dans la gestion des risques d'une organisation - Schéma issu de Position paper de l'IIA



Source : IIA POSITION PAPER - THE ROLE OF INTERNAL AUDITING IN ENTERPRISE-WIDE RISK MANAGEMENT - JAN 2009

Le Position Paper distingue trois catégories de tâches concourant à la gestion des risques d'une collectivité.

L'audit interne assure les tâches suivantes, selon les dispositions de la norme 2120 du CRIPP :

- Superviser le management des principaux risques ;
- Evaluer la communication des principaux risques ;
- Evaluer les processus de gestion des risques ;
- Donner l'assurance que les risques sont bien évalués ;
- Donner une assurance concernant les processus de gestion des risques.

Il appartient ainsi à l'audit interne de donner une assurance quant à la robustesse du système mis en place et le cas échéant de formuler toute recommandation visant à son amélioration.

L'audit interne contribue aux tâches suivantes, dans un cadre de responsabilité partagée :

- Faciliter l'identification et l'évaluation des risques ;
- Accompagner la direction dans le traitement des risques ;
- Coordonner la gestion globale des risques ;
- Centraliser la communication des risques ;
- Actualiser et développer le cadre de management des risques ;
- Promouvoir la mise en place d'un management des risques ;
- Elaborer une stratégie de management des risques pour arbitrage.

Dans ces domaines, l'audit interne borne son intervention à un rôle d'expertise et de conseil.

L'audit interne est enfin écarté des tâches suivantes, du fait d'un risque manifeste de conflits d'intérêts :

- Définir l'appétence pour le risque ;
- Imposer des processus de management des risques ;
- Décider de la manière de traiter les risques ;
- Mettre en œuvre des mesures de traitement des risques ;
- Prendre la responsabilité du management des risques ;
- Donner une assurance à la direction générale sur la gestion des risques.

Ces dernières tâches relèvent de la responsabilité du top management de l'organisation.

Fiche technique 16

Le tableau MARCI comme outil de pilotage des audits

Le tableau de type MARCI est un outil décisionnel utilisé pour la planification des travaux d'audit sur le fondement de la cartographie des risques de la collectivité.

Il contient les informations nécessaires pour positionner en priorité les travaux d'audit sur les risques porteurs d'enjeux majeurs et potentiellement non traités de manière appropriée.

En outre il remplit les fonctions suivantes.

Allocation optimale des moyens de contrôle

Le tableau MARCI permet d'identifier d'éventuels risques à faible criticité et fort degré de maîtrise.

Dans une logique de rationalisation de ses dépenses de fonctionnement, la collectivité peut avoir avantage à réduire les moyens de maîtrise attachés à ces risques particuliers et, le cas échéant, à les affecter à d'autres risques caractérisés par une criticité forte et des mesures de contrôle insuffisantes.

Grille de lecture pour distinguer les différents types d'audit

Dans la planification de travaux d'audit il peut être utile de distinguer plusieurs types d'audit afin de clairement spécifier leurs objets respectifs.

Même, si n'y a pas de nomenclature commune à l'ensemble des collectivités, on y retrouve généralement des audits assurantiels et des audits conseil ; or ces deux types missions peuvent être différenciées au regard des risques qu'elles traitent respectivement.

Les audits assurantiels concernent ainsi les risques à forte criticité et à fort degré de maîtrise.

Ils ont pour objet de vérifier la robustesse des mesures de maîtrise mises en place en réponse à ces risques et ainsi d'attester - ou corriger - le degré d'assurance susceptible d'être donné sur la capacité de la collectivité à contenir et le cas échéant surmonter les menaces inhérentes.

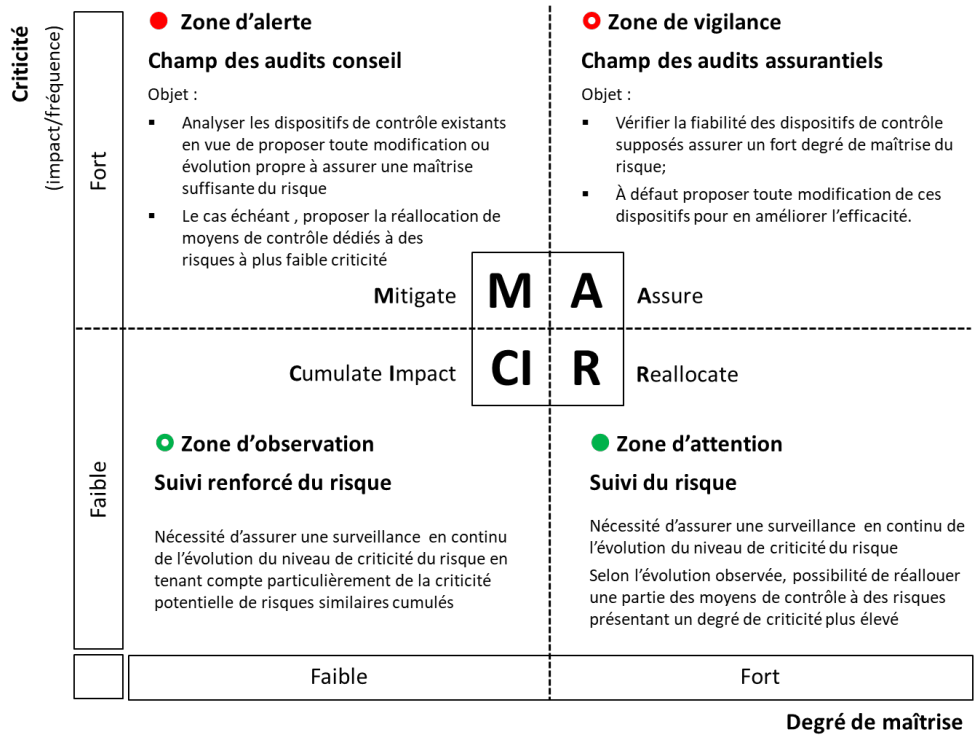
Les audits conseils sont quant à eux réalisés sur les risques à forte criticité et à faible degré de maîtrise.

Leur propos est de rechercher des voies pour réduire l'exposition de la collectivité à ces risques, au regard de l'enjeu qu'ils représentent pour la collectivité et des moyens de maîtrise susceptibles d'être mobilisés et/ou redéployés.

NB - Certaines collectivités conduisent également des « audits de conformité » qui visent à vérifier la correcte application de normes externes s'imposant dans un domaine particulier. Ces audits peuvent être assimilés à des audits assurantiels dans la mesure où ils donnent confirmation que les procédures existantes respectent - ou non - des prescriptions précisément définies ; ils sont en outre associés à des risques à forte criticité (puisque le non-respect de ces règles est en principe assorti de sanctions) et de par leur nature même sont présumés à fort degré de maîtrise.

Mode d'emploi d'un tableau MARCI

Pour les besoins de l'analyse, chaque risque y est positionné au regard des deux clés d'entrée : (1) la maîtrise du risque (2) la criticité du risque, qui combine l'impact du risque et la probabilité de survenance du risque.



Le support cartographique se divise en quatre espaces distincts :

- Mitigate (M) : il s'agit d'une zone d'alerte, la criticité de l'organisation au risque est forte et la maitrise faible. C'est le champ des audits conseil, il faut analyser les dispositifs de contrôle existants en vue de proposer des modifications ou évolutions tendant vers une assurance raisonnable du risque.
- Audit/assurance (A): il s'agit d'une zone de vigilance, la criticité de l'organisation au risque est forte et la maîtrise forte. C'est le champ des audits assurantiels, il faut vérifier la fiabilité des mesures de contrôle et en cas de faille proposer des modifications en vue d'en améliorer l'efficacité.
- Reallocate(R) : il s'agit d'une zone d'attention, la criticité de l'organisation au risque est faible et la maîtrise forte. C'est le champ de suivi du risque, il faut surveiller continuellement l'évolution de la criticité du risque et en cas de situation positive, réallouer des moyens de contrôle à d'autres risques présentant un degré de criticité plus important.
- Cumulate Impact (CI): il s'agit d'une zone d'observation, la criticité de l'organisation au risque est faible et la maîtrise faible. C'est le champ du suivi renforcé du risque, il faut assurer une surveillance en continu de l'évolution du niveau de criticité du risque en tenant compte particulièrement de la criticité potentielle des risques similaires cumulés

Fiche technique 17

Exemple de Fiche synthétique de suivi et de traitement d'un risque (criticité & maitrise)

Une collectivité engagée dans une entreprise de recensement et pilotage des risques afférents à son activité est amenée à déployer un outil de suivi permettant l'agrégation et l'exploitation de l'ensemble des données pertinentes.

A cet effet, il lui revient de créer des Fiches de suivi par risque propres à accueillir et conserver toute information susceptible de concourir à une démarche assurantielle globale fondée sur l'analyse des risques majeurs et la mise en place des mesures de maîtrise les mieux appropriées.

Ces Fiches de suivi doivent également être conçues de manière à assurer une parfaite traçabilité des travaux ayant conduit à la cotation de chaque risque tant en termes de criticité que de maîtrise ; la traçabilité ainsi créée doit être entière et continue à compter de la création du risque et de son positionnement dans la cartographie de la collectivité.

La mise en place d'un tel outil est un gage important de sérieux des travaux engagés et de robustesse du dispositif existant ; la collectivité peut en tirer profit pour renforcer son capital de confiance auprès de ses partenaires et des autres parties intéressées, de même elle sera ainsi en capacité d'extraire sans délai des éléments parfaitement tracés et assurés en réponse aux demandes de tout auditeur externe habilité.

Dans l'exemple qui suit, il est proposé de créer une **Fiche synthétique de suivi et de traitement** pour chaque risque identifié à l'échelle de la collectivité et éventuellement de ses organismes associés.

Selon les travaux menés pour conforter la démarche assurantielle de la collectivité, chaque Fiche **synthétique de suivi et de traitement** d'un risque déterminé a vocation à être complétée :

- d'une à plusieurs Fiche(s) de signalement d'un incident ;
- d'une à plusieurs de Fiche(s) de suivi de travaux de contrôle et d'audit ;
- d'une Fiche de suivi d'un plan d'action.

Le cas échéant, une Fiche additionnelle peut être ajoutée pour le suivi et le traitement des opportunités associées aux risques identifiées[164] ; cette fiche additionnelle se présenterait comme un décalque de la Fiche synthétique de suivi et de traitement des risques, sous réserve des deux points suivants :

- les opportunités seraient évaluées en termes de faisabilité et de valeur ajoutée pour la collectivité ;
- des plans d'action éventuellement conduits en réponse auront pour objet de renforcer leur faisabilité et/ou leur valeur ajoutée.

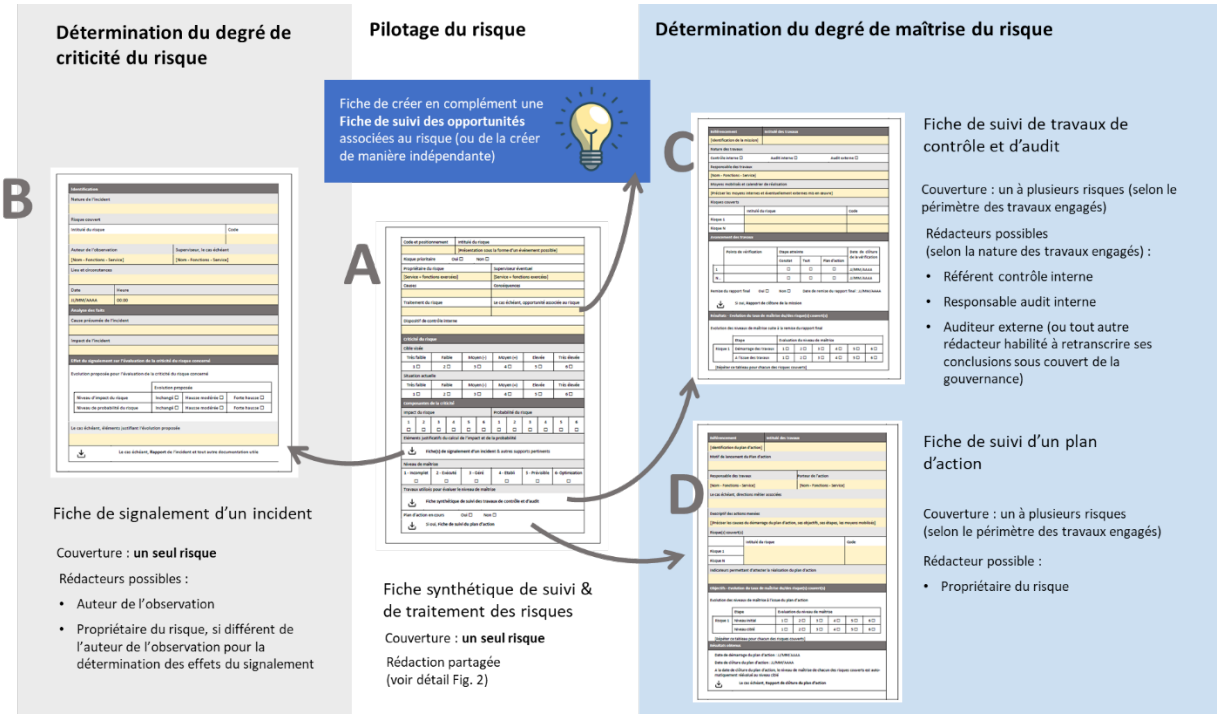
Une **codification unique des risques** doit permettre de rattacher ces Fiches l'une à l'autre et de les assembler dans une démarche de pilotage cohérente et parfaitement coordonnée.

Cette codification est à l'appréciation du manager des risques ; elle doit prendre appui sur l'arborescence des risques, telle qu'elle aura été établie et validée à l'échelle de la collectivité.

[164] Une collectivité peut également faire le choix de créer et renseigner des Fiches synthétique de suivi et traitement des opportunités distinctes des Fiches de risques entendus comme la seule possibilité de survenance d'événements négatifs

En complément, il convient d'établir un référencement rigoureux des missions de contrôle et d'audit ainsi que des travaux à la charge des directions métier (plans d'action) dès lors qu'ils contribuent à la détermination du niveau de maîtrise des risques de la collectivité ; la conduite de ce chantier préalable de classification et de normalisation des différents éléments constitutifs d'une démarche assurantielle globale est un gage fort de succès et de pérennité pour l'ensemble des parties engagées.

Fig. 1 Articulation des Fiches de suivi et pilotage d'un risque déterminé



Pour un pilotage optimal des risques associés à ses activités, une collectivité peut trouver avantage à acquérir ou développer en interne un Système d'information de gestion des risques (SIGR) couvrant l'ensemble des éléments constitutifs d'une démarche assurantielle globale.

Un tel outil doit permettre d'automatiser les liens entre ces différences et de faciliter les interactions entre l'ensemble des acteurs ayant part à la maîtrise des risques de la collectivité. Il a également vocation à produire des diagrammes décisionnels à destination de la Direction générale, de l'Exécutif ou de toute instance de pilotage et de suivi créée *ad hoc* ; ces supports doivent avoir pour effet d'améliorer la gouvernance du dispositif de maîtrise des risques en facilitant la représentation des progrès réalisés et des points de fragilité encore persistants.

Enfin, pour assurer l'auditabilité du système de gestion et de contrôle de la collectivité sur des périodes longues, il convient que le SIGR permette l'archivage :

- de l'ensemble des Fiches établies au titre des risques identifiés depuis le démarrage de chantier de cartographie et des Fiches de signalement d'événement prises en compte pour l'évaluation de leur criticité ;
- des Fiches descriptives des travaux de contrôle et d'audit couvrant le périmètre de ces risques ainsi que des Fiches descriptives des plans d'action menés en réponse à ces travaux ou indépendamment d'eux, y compris pour les missions clôturées et donc sans effet direct sur la note de maîtrise des risques de la collectivité.

Fiche synthétique de suivi & de traitement des risques identifiés

A

Code et positionnement	Intitulé du risque
❶	[Présentation sous la forme d'un événement possible]
Risque prioritaire ❷ Oui ☐ Non ☐	
Propriétaire du risque ❸	Superviseur éventuel
[Service + fonctions exercées]	[Service + fonctions exercées]
Causes	Conséquences
Traitement du risque	Le cas échéant, opportunité associée au risque
❹	❺
Dispositif de contrôle interne	
❻	

Criticité du risque

Cible visée ❼

Très faible	Faible	Moyen (-)	Moyen (+)	Elevée	Très élevée
1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐

Situation actuelle ❽

Très faible	Faible	Moyen (-)	Moyen (+)	Elevée	Très élevée
1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐

Composantes de la criticité

Impact du risque						Probabilité du risque					
1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐

Eléments justificatifs du calcul de l'impact et de la probabilité

Fiche(s) de signalement d'un incident & autres supports pertinents ❾

Niveau de maîtrise

1 - Incomplet	2 - Exécuté	3 - Géré	4 - Etabli	5 - Prévisible	6- Optimisation
☐	☐	☐	☐	☐	☐

Travaux utilisés pour évaluer le niveau de maîtrise ❿

Fiche synthétique de suivi des travaux de contrôle et d'audit

Plan d'action en cours ⓫ Oui ☐ Non ☐

Si oui, **Fiche de suivi du plan d'action**

Présentation générale

La **Fiche synthétique de suivi & de traitement** a pour objet de condenser en un seul point l'ensemble des éléments essentiels au pilotage de chacun des risques attachés au fonctionnement et à la mise en œuvre des politiques dont elle a la charge.

Pour chacun des risques identifiés, cette Fiche permet ainsi de déterminer :

- un niveau de criticité brut du risque couvrant son niveau d'impact et de probabilité en amont de toute mesure de maîtrise spécifique ;
- un niveau de maîtrise correspondant à l'efficience des moyens mobilisés pour maintenir sa criticité dans des limites acceptables par la collectivité ;
- un niveau de criticité net mesurant son niveau d'impact et de probabilité après prise en compte de l'effet des mesures de maîtrise spécifiques mises en œuvre.

Dans l'exemple qui suit,

- le niveau de criticité est mesuré sur une échelle de 1 à 6 ;
- le degré de maîtrise est également établi sur une échelle de 1 à 6, en référence à la nomenclature du COBIT 5[165].

Bien entendu, il appartient à chaque collectivité de choisir l'échelle la plus appropriée à ses besoins et aux attentes de la gouvernance.

La Fiche fait enfin apparaître les risques donnant lieu à un suivi prioritaire.

Le choix de ces risques appartient à la Direction générale et à la gouvernance ; il peut s'agir des risques présentant le niveau de criticité net le plus élevé et/ou de tout autre risque sélectionné en opportunité.

Contributeurs habilités

Le remplissage de la **Fiche synthétique de suivi & de traitement** revient pour l'essentiel au Manager des risques de la collectivité et au propriétaire du risque désigné.

Toutefois la direction générale et la gouvernance pourront intervenir ponctuellement pour fixer la criticité cible de chacun des risques et signaler ceux d'entre eux qui feront l'objet d'un suivi prioritaire.

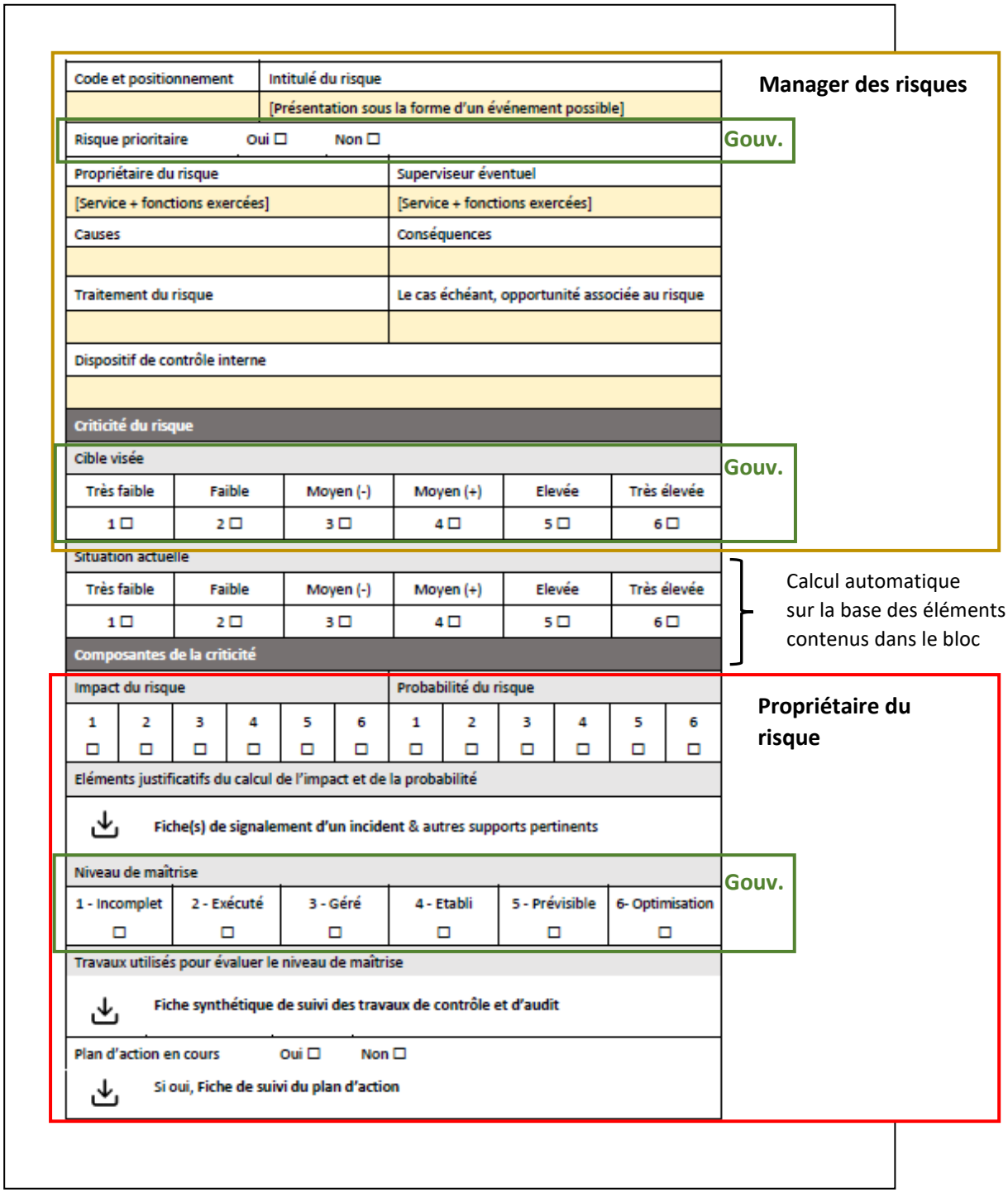
Les droits d'accès et de modification associés à ces différents profils doivent être établis en conséquence.

Voir en Figure 2 (ci-après) le détail des contributeurs susceptibles d'intervenir sur chacune des sections de la Fiche.

Chacune des Fiches est créée par le manager des risques. Elle est ensuite complétée et actualisée au fil de l'eau, en particulier pour rendre compte de tout événement susceptible de modifier le niveau de criticité ou de maîtrise du risque.

[165] Voir Fiche technique n° 13

Fig. 2 - Profils habilités à renseigner la Fiche de suivi & traitement



Légende

Gouv. Sous supervision directe de la direction générale et de la gouvernance

> Parties de la Fiche renseignées par le Manager des risques

Le manager des risques est habilité à renseigner les éléments suivants :

- désignation du risque et positionnement dans la cartographie des risques de la collectivité ;
- descriptif succinct du risque, en tant qu'événement déterminé par des causes particulières et entraînant des conséquences spécifiques ;
- traitement du risque, sous la forme des suites à donner (suppression du risque, maintien, transfert ou mutualisation ou mise en place de mesures de maîtrise proportionnées).

Le manager des risques est également amené à solliciter la direction générale et plus généralement la gouvernance en vue de l'attribution de chaque risque à un service métier dit « propriétaire du risque ».

> Parties de la Fiche renseignées par le propriétaire du risque

Une fois désigné par la direction générale, le propriétaire des risques a la responsabilité exclusive de renseigner les parties suivantes :

- détermination du niveau de criticité du risque (niveau initial ou niveau corrigé suite à la réalisation de plans d'action dédiés) ;
- signalement de tout incident en lien avec le risque ;
- spécification de tout plan d'action en cours visant à améliorer le degré de maîtrise du risque.

Par ailleurs, le propriétaire des risques est habilité à renseigner la part relative à l'évaluation du degré de maîtrise du risque :

- soit au titre de son appréciation initiale ;
- soit à l'issue d'un plan d'action conduit de la demande de la gouvernance dans le cas où la criticité nette initiale du risque est plus élevé que la criticité-cible ;
- soit pour faire suite aux recommandations d'une mission de contrôle ou d'audit relevant des seconde et troisième ligne de maîtrise ou enfin d'un audit externe.

> Parties de la Fiche renseignées sous la supervision directe de la gouvernance

La gouvernance et/ou la direction générale doit enfin pouvoir renseigner en dernier ressort les parties suivantes :

- identification des risques appelés à faire l'objet d'un suivi prioritaire[166] ;
- détermination du niveau de criticité ciblé (ou acceptable) pour chacun des risques[167].
- niveau de maîtrise du risque, en cas de divergence entre le propriétaire des risques et l'un ou l'autre des services en charge de la seconde ou de la troisième ligne de maîtrise des risques[168].

[166] Le choix de ces risques est entièrement discrétionnaire

[167] Selon l'appétence au risque de la collectivité

[168] Voir plus haut Section 3-B-2 (page 93)

Comment remplir la Fiche de suivi & traitement ?

Commentaire des points ❶ à ⓫ indiqués sur le modèle de Fiche.

❶ Attribuer un code unique à chaque risque qui permet de rattacher aisément le risque à une famille existante, en prenant sur appui sur les catégories du COSO-ERM, déclinées et adaptées selon l'arborescence mise en place à l'échelle de la collectivité

L'architecture de la cartographie des risques est à l'appréciation de la collectivité.

Elle vise à couvrir l'ensemble des aspects organisationnels, opérationnels et fonctionnels de son fonctionnement quotidien et de la mise en œuvre des politiques dont elle a la charge

> voir Fiche technique n° 10

❷ L'identification des risques prioritaires est du ressort de la Direction générale et de la gouvernance. Il s'agit des risques devant faire l'objet d'un suivi particulier, du fait de leur criticité et/ou de leur degré de maîtrise ou pour toute autre raison particulière.

❸ Le propriétaire du risque (« Contributeur métier ») est chargé de déterminer et éventuellement actualiser le degré de criticité du risque ; il lui revient également de fixer son niveau de maîtrise en tant que garant de la première ligne de maîtrise.

Le superviseur (« Responsable de domaine - Référent risques ») est un encadrant placé au-dessus du propriétaire du risque et responsable de la validation des données et évaluations proposées par ce dernier.

> voir Fiche technique n° 9

❹ Indiquer le traitement retenu à date :

- refus du risque - Abandon de l'activité porteuse de risque (dans ce cas les rubriques suivantes ne sont pas renseignées) ;
- réduction de la criticité du risque *via* la mise en œuvre d'un plan d'action (en cours) tendant un renforcement des mesures de maîtrise ;
- partage du risque par exemple par le biais de contrats de souscription d'assurance ;
- acceptation du risque en l'état, ce qui implique qu'aucun plan d'action n'est en cours pour réduire sa probabilité et/ou son impact.

Dans le cas où le choix est fait d'un partage du risque, préciser les modalités de partage ou de mutualisation mises en place.

Ces dispositions seront assimilées à des mesures de maîtrise ; le niveau de maîtrise du risque sera donc notamment établi au regard du niveau de couverture qu'elles sont susceptibles d'apporter.

Si la collectivité opte pour une réduction de la criticité du risque *via* la mise en œuvre d'un plan d'action, celui-ci est décrit dans une Fiche de suivi *ad hoc* (Fiche D).

❺ Le cas échéant, faire état des opportunités associées à ce risque.

On peut entendre par « opportunité » la possibilité de traiter ce risque non pas seulement de manière défensive mais de manière à favoriser la réalisation des objectifs de la collectivité sur le moyen et long terme, qu'il s'agisse d'objectifs stratégiques, opérationnels, financiers, informatiques, RH ou autres...

Ce point est conjointement renseigné par le manager des risques et la direction métier (propriétaire du risque) concernée.

Si la collectivité en fait le choix, l'opportunité liée au risque pourra être mesurée en termes de « faisabilité » et de « valeur ajoutée apportée ».

Leur évaluation respective sera réalisée sur une échelle à définir préalablement (par exemple sur une échelle croissante de 1 à 5).

De même, les opportunités priorisées par la Direction générale et la gouvernance pourront donner lieu à des plans d'action permettant de renforcer leur faisabilité et leur valeur ajoutée.

Pour documenter et tracer les éléments d'évaluation et de traitement propres à chacune des opportunités recensées, il peut être envisagé de créer une Fiche synthétique additionnelle (non proposée ici).

❻ Décrire le dispositif de contrôle interne associé à ce risque.

Il s'agit du premier niveau de maîtrise du risque, soit :

- les contrôles de routine réalisés par les agents opérationnels ;
- les surcontrôles ponctuels ou récurrents à la charge du management de proximité.

L'efficience et la robustesse de ces opérations peuvent être testées par le référent contrôle interne responsable du second niveau de maîtrise et le cas échéant dans le cadre d'audits assurantiels relevant du troisième niveau de maîtrise.

Dans le cas où un plan d'action en cours a pour objet de renforcer le dispositif de contrôle interne, il convient de décrire ici le dispositif actuel et non le dispositif ciblé.

❼ La criticité ciblée du risque net correspond à sa situation souhaitée à terme par la gouvernance.

Cette position est établie au regard des choix stratégiques de la collectivité et en tenant compte de son appétence au risque ; par souci de transparence et d'efficacité il est recommandé de procéder à ces arbitrages dans une instance dédiée telle qu'un Comité des risques.

NB- Si la criticité actuelle du risque est égale à la criticité ciblée, il n'y a lieu de mener aucune action additionnelle pour renforcer son degré de maîtrise, sous réserve bien sûr de changements ultérieurs dus à une dégradation de sa criticité brute ou à la mise en évidence de défaillances dans les mesures de maîtrise déployées.

❽ La criticité actuelle du risque résulte de la combinaison des trois composantes détaillées dans le bloc suivant :

- Impact du risque ;
- Probabilité du risque ;
- Niveau de maîtrise.

Il s'agit de donner une note composite sur la base des évaluations présentes données à ces trois composantes.

Il est recommandé d'utiliser pour ce faire un calcul automatique, à l'appréciation de la gouvernance.

La criticité actuelle du risque tient compte des mesures de maîtrise existantes[169].

Calcul de la criticité du risque

Il n'y a pas de méthode universelle ni même dominante pour le calcul de la criticité du risque.

Une option prudente peut être de retenir la plus haute valeur des trois valeurs contribuant au résultat demandé.

Il peut également être envisagé d'attribuer la moyenne de ces trois notes en arrondissant éventuellement par le haut.

Une autre solution serait d'attribuer une note mixte sur le seul périmètre de l'impact et de la probabilité (en retenant la plus haute ou une moyenne éventuellement arrondie des deux) et de la rapporter à la note de maîtrise, par exemple en la baissant d'un point si la note de maîtrise est de 3 («Géré») ou 2 («Exécuté») et de deux points si la note de maîtrise est seulement de 1 (« incomplet »).

De manière générale, ces calculs sont plus aisés à réaliser et à présenter si les trois composantes de la criticité sont évaluées sur une même échelle (ici de 1 à 6) mais il n'y a là aucun caractère d'obligation et d'autres formules peuvent être tout aussi légitimement adoptées.

❾ L'évaluation de la probabilité et de l'impact du risque a vocation à être vérifiée - et éventuellement corrigée - au regard des conclusions tirées des Fiche(s) de signalement de tout incident qui peut lui être rattaché.

Ces Fiches sont conservées et doivent être maintenues accessibles par ordre historique.

En outre et le cas échéant, indiquer le rattachement à la Norme ISO 31000 de la méthode retenue pour l'évaluation de l'impact et ou de la probabilité du risque.

Par souci de traçabilité, il convient de conserver l'ensemble des supports méthodologiques utilisés pour fixer la valeur attribuée (comptes-rendus d'entretiens, modélisation des causes et des effets, graphiques de flux, carnets d'enregistrement…)..

❿ Le niveau de maîtrise du risque est d'abord évalué au regard des mesures de maîtrise constatées au moment de son enregistrement.

Ce niveau peut être ultérieurement corrigé suite :

- à un plan d'action mené à l'initiative du propriétaire du risque (en particulier si la criticité cible du risque est en-deçà de sa criticité présente) ;
- à un plan d'action mené en réponse à des travaux de contrôle interne, à une mission d'audit interne / externe clôturée.

Le niveau de maîtrise retenu correspond à la note la plus récemment attribuée.

[169] Il peut également être fait mention de la criticité du risque brut - ou inhérent ou initial - qui ne tient pas compte des mesures de maîtrise en place. Dans ce cas, il est préférable de le noter distinctement dans la fiche (ce qui n'est pas le cas ici) - Voir supra Section 3-A-3 (page 76)

La date de validation des travaux pris en compte au titre de l'évaluation du niveau de maîtrise correspond à la date de remise des rapports finaux qui se rapportent à chacun d'entre eux.

La date de clôture de chacun de ces travaux doit ainsi être consignée de manière à conserver un historique du traitement du risque et à identifier sans risque d'erreur la note la plus récemment attribuée qui détermine son niveau de maîtrise actuel.

Pour écarter tout risque de confusion, les travaux ayant successivement contribué à la détermination du niveau de maîtrise peuvent être ainsi désignés :

- pour les missions de contrôle interne, d'audit interne ou d'audit externe clôturées, avec le numéro de référencement figurant dans la **Fiche de suivi de travaux de contrôle et d'audit** correspondante (Fiche C) ;
- pour les plans d'action clôturés, avec le numéro de référencement figurant dans la **Fiche de suivi d'un plan d'action** correspondante (Fiche D).

De même, par souci de transparence et de lisibilité, il peut être avantageux de faire figurer dans cette rubrique les missions de contrôle interne, d'audit interne ou d'audit externe en cours, dans la mesure où leurs résultats sont susceptibles de modifier à court terme le niveau de maîtrise du risque considéré.

Pour chacune de ces missions, il est ainsi proposé de préciser :

- leur degré d'avancement (mission non démarrée, mission en cours, mission clôturée) ;
- pour les missions clôturées, la date de remise du rapport final, de manière à faire d'abord apparaître les missions clôturées les plus récentes.

Point d'attention

Il convient d'assurer le pilotage de ce risque de manière différente selon les conclusions des contrôles et audits qui le concernent.

En effet, la direction générale et la gouvernance doivent être précisément averties de la précarité de toute note de maîtrise donnée par la direction métier dès lors qu'une mission de contrôle ou audit menée au titre de la seconde ou de la troisième ligne de maîtrise a émis des alertes (ou réserves) sur la fiabilité du dispositif existant et demandé qu'un plan d'action soit mené à bien en réponse.

Ces recommandations sont en principe accompagnées d'un échéancier indicatif de réalisation des actions attendues.

Dans le cas où la direction métier s'abstiendrait de conduire le plan d'action demandé dans les délais prescrits, la seconde ou la troisième ligne de maîtrise à l'origine de ces alertes (ou réserves) sera amenée à prendre son attache pour procéder à l'abaissement de la note de maîtrise du risque considéré.

En cas de désaccord entre la direction métier et la seconde ou la troisième ligne de maîtrise, la décision finale reviendra à la direction générale et la gouvernance.

Exemple - Travaux utilisés pour l'évaluation du degré de maîtrise d'un risque de fraude

Le présent exemple porte sur le niveau de maîtrise d'un risque de facturation frauduleuse *via* la possibilité d'achats auprès de fournisseurs factices, tel qu'évalué en septembre 2021.

A cette date, il convient de retenir la note attribuée en octobre 2020 par la direction métier suite à la clôture d'un Plan d'action qui faisait suite aux conclusions d'une précédente mission d'audit interne ; le dispositif issu de ce plan d'action est en cours de test par le référent contrôle interne.

L'ensemble de ces informations doivent se retrouver par ordre chronologique décroissant dans la rubrique « Travaux utilisés pour évaluer le niveau de maîtrise » de la Fiche synthétique de suivi & traitement établie au titre de ce risque.

Référence	Mission	Etat	Calendrier
CI/21/13	Evaluation du référent contrôle interne	En cours	Démarrage le 07/06/21 Clôture prévue en octobre 21
PA20/04	Plan d'action réalisé en réponse à l'audit interne (Réf. AI20/02)	Clos	Rapport remis le 15/10/2020 Détail accessible sur la **Fiche de suivi d'un plan d'action** (réf. PA20/40)
AI20/02	Audit interne sur la conformité des procédures d'achat	Clos	Rapport remis le 06/03/2020 Détail accessible sur la **Fiche de suivi de travaux de contrôle et d'audit** (réf. AI20/02)
NA	Evaluation initiale		Sans objet

⓫ Un plan d'action est exclusivement conduit à l'initiative du propriétaire du risque.

Il vise à une amélioration de la note de maîtrise actuelle.

Cette amélioration est chiffrée dés le lancement du plan ; elle est automatiquement appliquée dès que le plan est clôturé, sous réserve que les instances de contrôle en seconde et/ou troisième ligne de maîtrise invalident le changement de note opéré et ramènent le niveau de maîtrise à son état précédent voire plus bas encore[170].

Les plans d'action successivement menés doivent être archivés afin de conserver la pleine traçabilité des mesures prises en vue de la maîtrise du risque concerné.

[170] Bien entendu, leurs conclusions devront s'appuyer sur des travaux dûment documentés et menés selon les procédures en vigueur

Exemple de Fiche de signalement d'un incident

B

Identification		
Nature de l'incident		
Risque couvert ❶		
Intitulé du risque		Code
		❷
Auteur de l'observation	Superviseur, le cas échéant	
[Nom - Fonctions - Service]	[Nom - Fonctions - Service]	
Lieu et circonstances		
Date	Heure	
JJ/MM/AAAA	00:00	
Analyse des faits		
Cause présumée de l'incident		
❸		
Impact de l'incident		
❸		
Effet du signalement sur l'évaluation de la criticité du risque brut concerné		

Evolution proposée pour l'évaluation de la criticité du risque brut concerné ❹

	Evolution proposée		
Niveau d'impact du risque	Inchangé ☐	Hausse modérée ☐	Forte hausse ☐
Niveau de probabilité du risque	Inchangé ☐	Hausse modérée ☐	Forte hausse ☐

Le cas échéant, éléments justifiant l'évolution proposée

Le cas échéant, **Rapport** de l'incident et tout autre documentation utile

Présentation générale

Les **Fiches de signalement d'un incident** ont pour but d'assurer la traçabilité de l'ensemble des événements pertinents pour l'évaluation de la criticité d'un risque déterminé.

Chacune de ces Fiches est conçue pour recenser un événement passé qu'il convient de prendre en compte pour mesurer le niveau de probabilité et/ou d'impact d'un risque considéré.

Ainsi, il est tout à fait recevable, sinon souhaitable, de rattacher à un risque particulier - décrit dans une **Fiche synthétique de suivi & de traitement** *ad hoc* - plusieurs **Fiches de signalement d'un incident**, à raison d'une Fiche pour chacun des événements successivement retenus pour l'évaluation de sa criticité.

Les **Fiches de signalement d'un incident** doivent également pouvoir être renseignées de manière à rendre compte des causes et conséquences de chaque événement rapporté ; ces informations sont en effet susceptibles d'être utilement exploitées pour orienter de futurs contrôles relevant des trois lignes de maîtrise des risques.

Contributeurs habilités

Deux types de contributeurs sont habilités à renseigner une **Fiches de signalement d'un incident**, soit :

- le propriétaire du risque, qui remplit dans tous les cas les second et troisième volets relatifs respectivement à l'analyse des faits et à l'évaluation de l'effet du signalement sur le degré de criticité du risque concerné ;
- l'auteur de l'observation - s'il est différent du propriétaire du risque - qui a pour sa part seulement accès au premier volet contenant les différents éléments descriptifs nécessaires à la caractérisation de l'événement.

Comment remplir la Fiche de signalement d'un incident ?

Commentaire des points ❶ à ❹ indiqués sur le modèle de Fiche.

❶ Un même événement peut se rapporter à plusieurs risques.

Dans ce cas, il conviendra d'établir une Fiche de signalement distincte pour chacun de ces risques afin :

- d'adapter à leur contexte spécifique l'analyse des causes et conséquences de l'événement concerné ;
- de mesurer séparément ses effets sur leurs niveaux de criticité respectifs.

❷ Reprendre le code unique du risque auquel se rattache l'événement décrit, tel que figurant dans la Fiche correspondante (Fiche A).

❸ Les causes et impacts de l'incident doivent être décrits en lien avec les caractéristiques du risque auquel il se rattache.

Dans la Fiche synthétique qui le caractérise (Fiche A) le risque est en effet présenté comme un événement potentiel déterminé par des causes et conséquences particulières.

La description des causes et de l'impact de l'incident doit faciliter le repérage d'éventuels points de vulnérabilité dans la chaîne de traitement correspondante ; ces éléments doivent être pris en considération dans le cadre de contrôles ou d'audits diligentés ultérieurement, ils constituent des indications précieuses pour orienter les investigations sur la nature et l'importance des mesures correctrices requises.

❹ Il appartient au propriétaire du risque d'évaluer les effets de l'incident sur la criticité du risque brut concerné, mesurée tant en termes de probabilité que d'impact.

L'appréciation donnée revêt un caractère indicatif, cependant elle devra être prise en considération comme un élément de veille et d'alerte pour une possible actualisation immédiate ou à court terme du niveau de criticité qui lui a été attribué.

Le bien-fondé d'un tel ajustement doit être mesuré en lien avec d'éventuelles observations similaires réalisées postérieurement et/ou ultérieurement.

Pour objectiver et documenter son analyse, le propriétaire du risque peut également prendre appui sur l'une ou l'autre des méthodes de modélisation et de calcul recommandées dans la Norme ISO 31000 relative au management des risques

> voir Fiche technique n° 11

Exemple de Fiche de suivi de travaux de contrôle et d'audit

C

Référencement	Intitulé des travaux
[Identification de la mission] ❶	

Nature des travaux		
Contrôle interne ☐	Audit interne ☐	Audit externe ☐
Responsable des travaux ❷		
[Nom - Fonctions - Service]		
Moyens mobilisés et calendrier de réalisation ❸		
[Préciser les moyens internes et éventuellement externes mis en œuvre]		
Risques couverts ❹		

	Intitulé du risque	Code ❹
Risque 1		
Risque N		

Avancement des travaux ❺

	Points de vérification	Etape atteinte			Date de clôture de la vérification
		Constat	Test	Plan d'action	
1		☐	☐	☐	JJ/MM/AAAA
N…		☐	☐	☐	JJ/MM/AAAA

Remise du rapport final Oui ☐ Non ☐ Date de remise du rapport final : JJ/MM/AAAA

Si oui, **Rapport de clôture de la mission**

Résultats - Evolution du taux de maîtrise du/des risque(s) couvert(s) ❻

Evolution des niveaux de maîtrise suite à la remise du rapport final

	Etape	Evaluation du niveau de maîtrise					
Risque 1	Démarrage des travaux	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐
	A l'issue des travaux	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐

[Répéter ce tableau pour chacun des risques couverts]

Présentation générale

Une **Fiche synthétique de suivi et de travaux de contrôle et d'audit** distincte est créée pour documenter chaque mission menée à l'échelle de la seconde ou de la troisième ligne de maîtrise des risques.

Ces missions peuvent avoir pour objet d'évaluer le niveau de maîtrise d'un à plusieurs risques, selon le périmètre qu'elles recouvrent.

Une **Fiche de suivi des travaux de contrôle et d'audit** est ainsi conçue pour retracer l'ensemble des travaux relevant de la seconde et troisième ligne de maîtrise des risques - et éventuellement les travaux d'audit externe - ayant successivement contribué à déterminer le niveau de maîtrise attribué à un ou plusieurs risque(s) particulier(s).

Par conséquent, une même **Fiche de suivi des travaux de contrôle et d'audit** peut être rattachée à plusieurs Fiche(s) synthétique(s) de suivi et de traitement (Fiche A) dès lors que la mission décrite recouvre plusieurs risques et à raison d'une Fiche distincte pour chacun des risques concernés.

En retour, une Fiche synthétique de suivi et de traitement établie pour un risque particulier (Fiche A) peut renvoyer à plusieurs **Fiches synthétiques de suivi des travaux de contrôle et d'audit**, à raison d'une Fiche particulière pour chacun des travaux ayant tour à tour déterminé le niveau de maîtrise de ce risque.

A l'endroit du ou les risques qui lui sont associés, la Fiche synthétique remplit l'un des objectifs suivants :

- assurer la traçabilité d'une note de maîtrise corrigée - ou confirmée - suite à une mission de contrôle interne clôturée ;
- assurer la traçabilité d'une note de maîtrise corrigée - ou confirmée - suite à une mission d'audit interne clôturée ;
- assurer la traçabilité d'une note de maîtrise attribuée corrigée - ou confirmée - suite à une mission d'audit externe clôturée.

Son contenu doit offrir une vue synoptique de l'avancement des travaux et des conclusions obtenues ; il importe également d'y ajouter le rapport final de la mission dès lors que celui-ci est disponible, afin de marquer sa clôture et d'assurer une parfaite traçabilité des éléments concourant au pilotage assurantiel de la collectivité.

Contributeurs habilités

Chaque **Fiche de suivi des travaux de contrôle et d'audit** est créée et entièrement renseignée par le responsable de la mission considérée, qui peut être :

- le référent en charge du contrôle interne ;
- le responsable de l'audit interne ;
- tout auditeur externe habilité (ou un utilisateur interne désigné à cet effet).

Pour les missions relevant d'un auditeur externe, la **Fiche synthétique de suivi des travaux de contrôle et d'audit** afférente peut être renseignée par l'auditeur concerné ou tout autre contributeur désigné - par exemple le manageur des risques - sous la supervision de la gouvernance.

Comment remplir la Fiche de suivi de travaux de contrôle et d'audit ?

Commentaire des points ❶ à ❻ indiqués sur le modèle de Fiche.

❶ Le numéro de référencement de la mission permet de sécuriser son rattachement à/aux **Fiche(s) synthétique(s) de suivi et de traitement** (Fiche A) du des risques compris dans son périmètre.

Ce numéro est rappelé dans la rubrique « Travaux utilisés pour évaluer le niveau de maîtrise » de la ou des Fiches correspondantes.

❷ Le responsable des travaux est également le signataire du rapport produit au terme de la mission.

❸ S'agissant des moyens mobilisés, faire état des qualifications des contrôleurs / auditeurs missionnés ainsi que de leur expertise dans les domaines considérés[171].

❹ Une mission de contrôle ou d'audit peut couvrir un ou plusieurs risques.

Le périmètre de la cartographie des risques couvert spécifiquement par chaque mission doit être spécifié préalablement au démarrage des travaux.

Pour écarter toute possibilité de confusion, le ou les risques couverts par les travaux décrits dans la présente Fiche doivent être identifiés par leur codification spécifique, telle qu'elle apparaît dans la Fiche synthétique de suivi & de traitement se rapportant à chacun d'entre eux (voir Fiche A - point ❶).

❺ Cette rubrique est renseignée pour l'ensemble de la mission de contrôle ou d'audit.

Elle vise à rendre compte de l'avancement des travaux et à visualiser les suites données aux différents points de vérification.

Pour chacun d'entre eux, trois étapes sont proposées : (1) Constat (2) Test et (3) Plan d'action.

L'étape de Constat correspond à la documentation du process et à l'identification des points de vulnérabilité éventuels qui pourraient appeler en réponse des mesures correctrices ciblées.

L'étape de Test consiste en une vérification de la robustesse et de la fiabilité des points de contrôle existant au travers de l'analyse de conformité de la chaine de traitement (pointage des pièces, analyse des outputs…) et cela sur la base de l'exhaustivité des données disponibles ou d'un échantillon représentatif établi par sondage.

L'étape relative au Plan d'action est mise en œuvre si les étapes « constat » et « test » n'aboutissent pas à des résultats conclusifs et mettent au contraire en évidence des défaillances suffisamment significatives pour justifier une révision plus ou moins étendue du process et une reprise de tout ou partie des opérations déjà réalisées ou en cours. Dans ce cas, le responsable de la mission de contrôle ou d'audit appelle le service métier concerné à mener à bien un plan d'action propre à corriger au plus tôt les dysfonctionnements relevés.

[171] Voir notamment à cet égard la Norme 1200 du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP) relative à la compétence et à la conscience professionnelle des intervenants

❻ Cette rubrique vise à formaliser les éventuels ajustements apportés à la note de maîtrise du ou des risques couverts par les travaux de contrôle ou d'audit, suite à leur clôture et à la remise du rapport final.

Pour chacun des risques concernés, il convient de rapporter :

- le niveau de maîtrise en phase de démarrage, correspondant à la note consignée dans la **Fiche synthétique de suivi & de traitement** à la date de lancement des travaux ;
- le niveau de maîtrise confirmé ou éventuellement ajusté à la baisse au terme de la mission.

La date de démarrage des travaux correspond à la date de signature de la notification de la mission (courrier ou note à l'attention du responsable de la mission…).

La date validation des travaux correspond à la date de remise du rapport final de la mission.

Une mission de contrôle ou d'audit est ainsi réputée close lorsque l'ensemble des vérifications initialement prévues ont été menées jusqu'en phase « Test » ou « Plan d'action ».

La date de clôture de la dernière vérification en phase « Test » ou « Plan d'action » correspond à la date de clôture de la mission[172].

La date de remise du rapport final est concomitante avec la date de clôture de la mission ou postérieure.

Pour une même mission, les dates de démarrage et de clôture des travaux sont identiques pour l'ensemble des risques couverts.

Il est enfin recommandé de donner accès en téléchargement au rapport final remis à l'issue de la mission en vue d'une traçabilité maximale des travaux réalisés.

La Fiche de suivi établie pour chaque mission de contrôle ou d'audit a vocation à être désactivée dès la clôture de la mission qu'elle a pour objet de décrire ; à compter de ce moment, elle passe en statut d'archivage.

[172] Lorsqu'une vérification aboutit à la phase « Plan d'action », la date de validation associée ne correspond pas à la date de réalisation du plan d'action - qui est dans tous les cas à l'appréciation du service métier - mais à la date de formalisation de la recommandation, laquelle correspond à la date de remise du rapport final.

Exemple de Fiche de suivi d'un plan d'action

D

Référencement ❶	**Intitulé des travaux**
[Identification du plan d'action]	

Motif de lancement du Plan d'action ❷

Responsable des travaux ❸	Porteur de l'action ❹
[Nom - Fonctions - Service]	[Nom - Fonctions - Service]

Le cas échéant, directions métier associées ❺

Descriptif des actions menées
[[Préciser les causes du démarrage du plan d'action, ses objectifs, ses étapes, les moyens mobilisés]

Risque(s) couvert(s) ❻

	Intitulé du risque	Code
Risque 1		
Risque N		

Indicateurs permettant d'attester la réalisation du plan d'action ❼

Objectifs - Evolution du taux de maîtrise du/des risque(s) couvert(s) ❽

Evolution des niveaux de maîtrise à l'issue du plan d'action

	Etape	Evaluation du niveau de maîtrise					
Risque 1	Niveau initial	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐
	Niveau ciblé	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐

[Répéter ce tableau pour chacun des risques couverts]

Résultats obtenus ❾

Date de démarrage du plan d'action : JJ/MM/AAAA

Date de clôture du plan d'action : JJ/MM/AAAA

A la date de clôture du plan d'action, le niveau de maîtrise de chacun des risques couverts est automatiquement réévalué au niveau ciblé

Le cas échéant, **Rapport de clôture du plan d'action**

Présentation générale

La **Fiche de suivi d'un plan d'action** a pour objet de retracer l'ensemble des travaux susceptibles d'être engagés par le propriétaire du risque (direction métier) pour améliorer son degré de maîtrise et réduire de la sorte sa probabilité et/ou son impact potentiel.

Un plan d'action peut couvrir un ou plusieurs risques.

Une même **Fiche de suivi d'un plan d'action** peut ainsi être rattachée à plusieurs Fiche(s) synthétique(s) de suivi et de traitement (Fiche A) dès lors que les travaux engagés concernent plusieurs risques et à raison d'une Fiche distincte pour chacun des risques concernés.

En retour, une Fiche synthétique de suivi et de traitement établie pour un risque particulier (Fiche A) peut renvoyer à plusieurs **Fiches de suivi d'un plan d'action**, à raison d'une Fiche particulière pour chacun des Plans d'action ayant successivement déterminé le niveau de maîtrise de ce risque.

La **Fiche de suivi d'un plan d'action** doit être établie pour rendre un compte précis des travaux réalisés, en particulier au regard des trois points suivants :

- faits générateurs de la mise en œuvre de ce Plan d'action, lesquels peuvent être la réponse apportée aux conclusions d'une mission particulière de contrôle ou d'audit mais aussi une demande de la gouvernance liée à l'identification du risque ou inscrite dans une démarche assurantielle globale ;
- noms et fonctions des agents responsables de la conduite et de la validation des travaux ;
- indicateurs pris en compte pour attester que le plan d'action a été effectivement mené à bien et que les objectifs fixés en termes de maîtrise des risques ont été réalisés.

La conservation de ces éléments contribuera à une parfaite auditabilité du système de gestion et de contrôle de la collectivité sur le long terme.

Contributeurs habilités

Le plan d'action ainsi conçu est conduit sous l'entière responsabilité de la direction métier concernée (propriétaire du risque), à charge pour le référent contrôle interne et/ou le responsable de d'audit interne de s'assurer ultérieurement - et en toute indépendance - de la robustesse et de l'efficience du nouveau dispositif qui en résulte.

Dans le cas où un plan d'action couvre des risques relevant de différentes directions métier (propriétaires de risques) il conviendra d'identifier une direction métier assurant son chef-de-file.

Il reviendra à cette direction métier chef-de-file de produire un rapport global pour le plan d'action et de s'assurer que les directions métier associées donnent leur acquiescement à ses conclusions.

Comment remplir la Fiche de suivi d'un plan d'action ?

Commentaire des points ❶ à ❾ indiqués sur le modèle de Fiche.

❶ Le numéro de référencement de la mission permet de sécuriser son rattachement à/aux **Fiche(s) synthétique(s) de suivi et de traitement** (Fiche A) du des risques compris dans son périmètre.

Ce numéro est rappelé dans la rubrique « Travaux utilisés pour évaluer le niveau de maîtrise » de la ou des Fiches correspondantes.

❷ Le plan d'action peut être mis en œuvre à l'issue :

- à l'initiative du propriétaire du risque, sur proposition de la gouvernance ;
- suite aux recommandations d'une mission de contrôle interne clôturée ;
- suite aux recommandations d'une mission d'audit interne clôturée ;
- suite aux recommandations d'une mission d'audit externe clôturée.

Ces cas de figure correspondent aux « motifs » susceptibles d'être retenus.

Si le plan d'action répond à une demande particulière de la gouvernance, celle-ci est en principe concomitante de la détection du risque et peut représenter la réponse concrète apportée au traitement proposé, si le choix a été fait d'une Réduction de la criticité du risque (voir la Fiche A - point ❹).

Toutefois, la mise en œuvre d'un plan d'action peut également être demandée par la gouvernance à une date ultérieure s'il apparaît que la criticité nette du risque est à ce moment plus élevée que sa criticité nette ciblée (voir la Fiche A - point ⓫).

Dans le cas où le plan d'action fait suite aux recommandations d'une mission de contrôle interne clôturée, d'une mission d'audit interne clôturée ou d'une mission d'audit externe clôturée, sa date de lancement doit être postérieure à la date de remise du rapport final de la mission concernée. De même et afin d'écarter toute possibilité de confusion, il est opportun de rappeler le numéro de référencement de la mission de contrôle et d'audit à l'origine du Plan d'action (voir la Fiche C - point ❶).

❸ Le responsable des travaux appartient nécessairement à la direction métier propriétaire du risque.

Dans le cas où le plan d'action couvre plusieurs risques relevant de différentes directions métier, le responsable des travaux est à identifier dans la direction métier assurant le chef-de-filat du plan d'action.

❹ Mentionner le porteur de l'action s'il est différent du responsable des travaux.

Faire état de ses noms et fonctions.

❺ Si le plan d'action est étendu à des risques rattachés à plusieurs directions métier, mentionner ici les directions métier associées à la conduite des travaux sans en assurer le chef-de-file.

❻ Dans le souci de leur correct rattachement, le ou les risques couvert(s) par le plan d'action doivent être identifiés par leur codification spécifique, telle qu'elle apparaît dans la Fiche synthétique de suivi & de traitement se rapportant à chacun (voir Fiche A - point ❶).

❼ Les indicateurs de réalisation permettent de vérifier que le plan d'action a été effectivement mené à terme ; dès lors qu'ils sont remplis, le propriétaire du risque est fondé à clôturer le plan d'action et à réévaluer le niveau de maîtrise du risque à hauteur de la cible fixée.

Ces indicateurs doivent être établis en amont du démarrage du plan d'action.

❽ Dans le présent exemple, le niveau de maîtrise ciblé pour chacun des risques compris dans le plan d'action est évalué selon une échelle de 1 à 6.

Le niveau visé est nécessairement supérieur au niveau de maîtrise actuel du risque.

Ce niveau de maîtrise ciblé ne pourra être enregistré et entériné qu'à compter de la clôture du plan d'action en cours.

❾ La date de clôture du plan d'action coïncide avec la remise d'un rapport final de réalisation.

Ce rapport est établi et validé par la direction métier propriétaire du risque, le cas échéant avec l'assentiment explicite des directions métier associées.

Il y est notamment fait mention du niveau d'exécution des indicateurs de réalisation initialement associés au plan d'action qui permet d'attester la pleine atteinte des objectifs fixés et donc d'entériner les résultats attendus.

La Fiche de suivi est désactivée dès la clôture du plan d'action qu'elle a pour objet de décrire ; à compter de ce moment, elle passe en statut d'archivage.

Bibliographie

Sources utilisées pour le présent ouvrage

Carassus, D. (2020). *Le pilotage des politiques publiques locales : De la planification à l'évaluation*. Berger-Levrault.

Le Nocher, B. (2020). *Le paradoxe de la transparence financière dans les collectivités : Un enjeu ancien, une mise en œuvre récente*

Potier, V. (2020). *Guide pour la bonne gestion des collectivités territoriales*. *36*(2532).

Wolf, O. (2020). 40 ans d'analyse financière dans les collectivités décentralisées. *Gestion & Finances Publiques*, *5*(5), 18-27. Cairn.info.

Cour des comptes. (2019). *Bilan intermédiaire de l'expérimentation de la certification des comptes locaux*

Institut français de l'audit et du contrôle internes & Conférence des inspecteurs et auditeurs territoriaux & PwC (2019). *Maîtrise des risques dans les collectivités territoriales*

Sutra, G. (2018). *Management du risque, une approche stratégique : Cartographie des risques, prenez de la hauteur ! ISO 31000*. Afnor éditions

Desroches A., Aguini N., Dadoun M., Delmotte S.; Editions Lavoisier (2016) *Analyse globale des risques - 2ème édition*

Ettourki, M. (2016). *Dispositif de controle interne et de gestion des risques comme cadre de l'intégrité- Expérience de l'ONEE-Branche eau*

Mortureux, Y. (2016). Fondamentaux de l'analyse de risque, regard fiabiliste sur la sécurité industrielle. *Regard sur la sécurité industrielle*, *2*

DGFiP. (2010). *Echelle de maturité de la gestion des risques*

Institut français de l'audit et du contrôle internes (Éd.). (2006). *L'audit interne et le management des collectivités territoriales : La cartographie des risques*. IFACI.

Fédération of European risk management associations. (2003). *Cadre de référence de la gestion des risques*.

Lectures complémentaires recommandées

Kozyrkov, C. (2021). Investir dans l'analytique pour identifier les risques plus tôt. *Harvard Business Review*, 55-57.

Suarez, F. F., & Montes, J. S. (2021). Développer la résilience organisationnelle. *Harvard Business Review*, 48-54.

Prévalet, M. (2020). *La gestion des risques dans la Fonction publique : Gestion de crise dans une direction ou un service*.

Bontems, T., & Goulin, S. (2017). *Modéliser les vulnérabilités : AVoID : Une approche hyper cubique de la vulnérabilité au profit de la prise de décision.* Qualita2017 : 12ème Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable, Bourges. https://halshs.archives-ouvertes.fr/halshs-01590749/document

Institut français de l'audit et du contrôle internes (2017). *Le management des risques de l'entreprise Une démarche intégrée à la stratégie et à la performance Synthèse*. https://docs.ifaci.com/wp-content/uploads/2018/03/COSO-ERM-2017-synthe-se.pdf

Beck, U. (2015). *La société du risque : Sur la voie d'une autre modernité*.

Darsa, J.-D. (2015). *Le facteur risque de l'entreprise : Méthode inédite de mesure des risques de l'entreprise*.

Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, S., Salamasick, M., Riddle, C., & Institut français des auditeurs consultants internes. (2015). *Manuel d'audit interne : Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles.

Institut français de l'audit et du contrôle interne & PricewaterhouseCoopers. (2014). *Coso référentiel intégré de contrôle interne : Principes de mise en oeuvre et de pilotage*. Eyrolles.

Louisot, J.-P. (2014). *Gestion des risques*. http://res.banq.qc.ca/login?url=http://www.numilog.com/bibliotheque/bnquebec/fiche_livre.asp?idprod=463831

Raimbault, P., & Cultiaux, D. (2014). *Les cadres publics et l'État de droit : Prévenir les risques juridiques*. Canopé éd.

Les graphiques et illustrations suivants ont été réalisés au titre de la présente publication[173] :

Page 30	Périmètre de l'exercice de cartographie
Page 56	Représentation matricielle des risques en tant qu'opportunités
Page 67	Cheminement de l'identification à la maîtrise des risques
Page 83	Cartographie des risques dans un processus de management stratégique et assurantiel
Page 84	Chaine de traitement du risque
Page 98	Proposition de phasage pour la mise en œuvre d'une démarche assurantielle à l'échelle d'une collectivité
Page 147	Calendrier de l'expérimentation de la certification des comptes
Page 186	Utilisation des outils & méthodes proposés dans la norme ISO 31000 aux différentes étapes du déploiement d'une fonction de management des risques
Page 226	Présentation d'un tableau MARCI

Edité en janvier 2022

[173] Le graphique en page 83 a été réalisé par Franck VILLOT. Les graphiques en pages 67 et 84 ont été réalisés par Olivier WATEL, Les graphiques en pages 30, 56, 98, 147, 186 et 226 ont été réalisés par Stéphane LABONNE

À propos

Porte-paroles de la profession d'audit interne, l'Institut Français d'Audit et de Contrôle internes (IFACI) et l'Institut des auditeurs internes (IIA) sont des autorités reconnues dans le domaine de la formation et de la formulation des normes, lignes directrices et certifications.

Copyright

Le copyright de ce guide pratique est détenu par l'IFACI.
Pour l'autorisation de reproduction, prière de contacter l'IFACI à l'adresse suivante :
institut@ifaci.com

IFACI

98bis, Boulevard Haussman
75008 PARIS, France
Téléphone : 01 40 08 48 00
Fax : 01 40 08 48 20
Site Web : www.ifaci.com
Courrier électronique : institut@ifaci.com

ifaci
institut français de l'audit et du contrôle internes

GROUPE PROFESSIONNEL
COLLECTIVITÉS TERRITORIALES

DE LA CONNAISSANCE À LA MAÎTRISE DES RISQUES DANS LES COLLECTIVITÉS LOCALES

Institut Français de l'Audit et du Contrôle Internes -
98bis, Boulevard Haussmann 75008 Paris - Tél. : +331 40 08 48 00 - institut@ifaci.com