Les Cahiers techniques

Le partage de tous les savoirs

ISSN : 1950-0033 – ISBN : 979-10-92310-02-3 - 20€ - N° 14 - Juin 2015

Déployer un dispositif de maîtrise des risques et de Contrôle Interne au sein des organismes publics :

Approche pratique en complément du Livre Blanc précédent « La gestion des risques et le contrôle interne dans les collectivités territoriales »

Groupe Services Publics

Les Cahiers techniques

Le partage de tous les savoirs

Déployer un dispositif de maîtrise des risques et de Contrôle Interne au sein des organismes publics :

Approche pratique en complément du Livre Blanc précédent « La gestion des risques et le contrôle interne dans les collectivités territoriales »

ASSOCIATION NATIONALE
DES DIRECTEURS FINANCIERS
ET DE CONTRÔLE DE GESTION

LA DFCG, L'ASSOCIATION DES PROFESSIONNELS FINANCE-GESTION

ASSOCIATION NATIONALE
DES DIRECTEURS FINANCIERS
ET DE CONTRÔLE DE GESTION

Groupe Services Publics

n°1
des associations
des professionnels
finances-gestion

3 000
membres

1 700
sociétés
représentant
1/3 du PIB
de la France

Plus de 50
ans
d'existence

EN 50 ANS, LA DFCG EST DEVENUE UN RÉFÉRENT DANS LA SPHÈRE FINANCIÈRE

En 1964 a été créée l'ANCG, l'Association Nationale des Conseillers et Contrôleurs de Gestion. Après quelques années d'existence marquées par un fort développement du métier de "contrôleur" et le lancement de l'Association Internationale (IAFEI), elle a décidé d'adopter le nom d'Association Nationale des Directeurs Financiers et de Contrôle de Gestion dont le sigle est DFCG.

Aujourd'hui, la DFCG est une association de professionnels - Directeurs Financiers et/ou Directeurs de Contrôle de Gestion - d'entreprises privées ou publiques. Des enseignants et des conseils d'entreprises dans les domaines de la gestion, des finances et des systèmes d'information en sont également membres. Elle accueille les jeunes professionnels se destinant au plus haut niveau de la profession au sein du club DFCG Avenir.

LA DIFFÉRENCE COMME SOURCE D'ENRICHISSEMENT

L'Association compte quelques 3 200 membres répartis dans tous les secteurs économiques et géographiques du pays. La DFCG regroupe toutes les tailles d'entreprises, depuis la PME jusqu'aux grands groupes internationaux. À l'image du tissu économique français, une forte proportion de PME et ETI est représentée par ses directeurs administratifs et financiers ou directeurs finance-gestion. Cette diversité est une formidable source d'échange d'expériences et d'enrichissement des débats.

EXCELLER DANS NOS MISSIONS

- **ENRICHIR** professionnellement ses membres, par l'échange d'idées et d'expériences, dans le cadre de manifestations et de formations, par la publication de sa revue Finance&Gestion et du blog Vox Fi, par les travaux de son Comité Scientifique.
- **OUVRIR** à chaque membre la richesse du réseau DFCG, structuré en groupes régionaux et en groupes sectoriels pour plus de proximité.
- **INTERNATIONALISER** nos contacts avec les associations similaires à l'étranger, notamment au sein de l'International Association of Financial Executives Institutes (IAFEI).
- **INTERVENIR** sur les problématiques comptables et financières en concertation étroite avec les associations professionnelles de la finance telles que l'APDC (Association des Professionnels et Directeurs Comptabilité et Gestion), l'AFIGESE (Association Finance - Gestion - Évaluation des Collectivités Territoriales), l'AFDCC (Association des Crédit Managers), l'AFTE (Association Française des Trésoriers d'Entreprise), l'IFACI (Institut Français de l'Audit et du Contrôle Internes), l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise), l'IFA (Institut Français des Administrateurs), EOA (European Outsourcing Association).
- **SUSCITER** la réflexion et le travail en commun pour faire émerger des pôles d'expertise, permettant à la DFCG d'être un acteur de référence dans le débat économique et financier.
- **ACCUEILLIR** ses membres dans un espace de convivialité, dans un réseau professionnel et solidaire. C'est également la possibilité d'intégrer plus rapidement la communauté financière et de progresser dans son quotidien avec une attention particulière portée sur la gestion de carrière.
- **ÉCHANGER** des expertises métiers complémentaires dans le cadre de la Maison de la Finance. Cette « Maison de la Finance », regroupant l'AFDCC, l'APDC et la DFCG, est une première initiative dans le monde associatif professionnel et permet, dès à présent, à tous les collaborateurs des services financiers des entreprises de se retrouver sous un même toit avec une panoplie complète de services et conseils pour les accompagner au quotidien dans le développement de leurs compétences : formations, ressources documentaires, événements, groupes de travail, commissions métier.

ILS ONT PILOTÉ CE CAHIER

PRÉSENTATION DU GROUPE SERVICES PUBLICS

Créé au début de l'année 1994, le Groupe Services Publics se propose de réunir les dirigeants Finance-Gestion des services publics et des collectivités territoriales. Le groupe "Services Publics" comprend des responsables de l'administration centrale (civile et militaire), des établissements publics à caractère administratif, industriel et commercial, des organismes de sécurité sociale et des caisses de mutualité sociale agricole, ainsi que des directeurs financiers et de contrôle de gestion des collectivités territoriales.
Le Groupe est présidé par Emmanuel Millard, Directeur des Finances et du Contrôle Interne, des Achats et des Affaires Juridiques d'Universcience, Etablissement Public de la Cité des Sciences et de l'Industrie, de la Géode et du Palais de la Découverte.

Son but est de promouvoir les nouveaux concepts et méthodes de gestion dans les Services Publics :

- Par la réalisation d'études au sein de groupes thématiques,
- Par le développement des échanges entre responsables finances gestion, des services publics d'une part et des entreprises privées d'autre part,
- Par la communication d'expériences innovantes dans le domaine Finance-Gestion,
- Par l'organisation de manifestations de très haute tenue abordant des thématiques finances gestion des services publics.

La DFCG remercie vivement les équipes de CGI Business Consulting pour leur implication dans le groupe de travail ayant abouti à la réalisation de ce livre blanc.

CGI | Business Consulting

PRÉSENTATION DE CGI BUSINESS CONSULTING

CGI Business Consulting, cabinet de conseil en innovation et transformation, fait partie du Groupe CGI inc. Ses consultants associent expertises sectorielles, fonctionnelles et technologiques pour accompagner les plus grandes entreprises et organisations. Parce que chaque client est unique, CGI Business Consulting a créé des méthodes de travail spécifiques permettant à chacun de prendre part au management de sa transformation et garantissant une amélioration durable de ses performances. Fondé en 1976, Groupe CGI inc. est la cinquième plus importante entreprise indépendante de services en technologies de l'information et en gestion des processus d'affaires au monde.

Avec environ 68 000 membres répartis dans ses bureaux et centres mondiaux de prestation de services dans les Amériques, en Europe et en Asie-Pacifique, CGI offre un portefeuille complet de services, y compris des services-conseils stratégiques en informatique et en management, des services d'intégration de systèmes, de développement et de maintenance d'applications informatiques, de gestion d'infrastructures technologiques ainsi qu'une vaste gamme de solutions exclusives. À la suite de la récente acquisition de Logica, CGI génère désormais des revenus annualisés de plus de 7 milliards d'euros et la valeur estimée de son carnet de commandes s'élève à environ 13 milliards d'euros.

Les actions de CGI sont inscrites à la Bourse de Toronto (GIB.A) ainsi qu'à la Bourse de New York (GIB) et figurent dans l'indice FTSE4Good.

Site Web : www.cgi.com

COMPOSITION
du groupe de travail

Membres du groupe de travail :

Philippe Baron, Vice Président du Groupe Services Publics DFCG et Partner CGI Business Consulting

Benedikt Cordt-Møller, Directeur du service du contrôle interne du Département de la solidarité et de l'emploi, Etat de Genève

Raymond Marfaing, Directeur Adjoint de l'audit et des risques, Groupe SNCF

Alain Scordel, DAF Institut Polytechnique de Grenoble

Aline Autissier, Responsable administrative, Cellule Prospective, Evaluation, Ressources, Université de la Rochelle

Clarisse Renault, Consultante

Geoffroy Laine, Responsable Contrôle Interne, Ubifrance

Hélène Barrios, Directrice Générale, Cegid Public

Régis Baudouin, Secrétaire Général, Cegid Public

Pascale Gramain, Secrétaire générale du Cancéropôle Île-de-France

Philippe Germak, CNAM

Les équipes de CGI Business Consulting

PRÉFACE

par ***Didier Migaud***,
Premier président de la Cour des comptes

La Constitution dispose que « les comptes des administrations publiques sont réguliers, sincères et donnent une image fidèle de leur gestion, de leur patrimoine et de leur situation financière ».

En application des dispositions du code des juridictions financières, la Cour des comptes s'assure de la qualité des comptes des administrations publiques. Elle les certifie elle-même, dans le cas de l'État et du régime général de la sécurité sociale. En ce qui concerne certains établissements publics dont les comptes sont soumis à certification, elle rend compte des certifications assurées par les commissaires aux comptes. Pour l'exercice 2013, trois quarts des charges brutes globales des administrations publiques ont été auditées, soit par la Cour, soit par un commissaire aux comptes.

La Cour a eu l'occasion de rappeler, dans son rapport public annuel 2015, qu'une part significative de ses constats se concentrait sur l'évaluation du contrôle et de l'audit internes : « au regard de la volumétrie des opérations effectuées, la qualité des comptes est subordonnée à la mise en place d'un dispositif de contrôle interne permettant de prévenir, détecter et corriger en temps voulu une anomalie de portée significative affectant les opérations effectuées et comptabilisées […] La Cour examine aussi l'audit interne, qui doit permettre de vérifier l'effectivité du contrôle interne et d'apprécier son efficacité ». Ce faisant, la Cour dispose d'un puissant levier de modernisation de la gestion des organismes publics.

Ainsi, pour l'État, le contrôle interne a progressé d'abord sous l'effet de la certification des comptes par la juridiction financière. L'auteur de la LOLF que je suis, avec Alain Lambert, est d'ailleurs particulièrement attaché à cet exercice, qui amène chaque année la Cour des comptes, depuis bientôt dix ans, à produire l'acte de certification des comptes de l'État. En tant que Premier président, je veille à ce que ces travaux permettent de porter une vision d'ensemble de l'État et de ses opérateurs. C'est d'ailleurs pour couvrir l'ensemble des départements ministériels que l'élaboration de l'acte est confiée à une formation inter chambres de la Cour.

Lorsque la Cour a rendu public l'acte de certification des comptes de l'État pour 2013, elle a appelé les pouvoirs publics à concentrer les travaux d'amélioration sur les cinq réserves « substantielles » qui demeuraient. Parmi ces réserves, la deuxième concernait les dispositifs ministériels de contrôle interne et d'audit interne, considérés comme encore trop peu effectifs et efficaces. Lors de la présentation de ce travail aux parlementaires, je soulignais pourtant le paradoxe de cette situation, alors que le développement de ces fonctions répond aux besoins de chaque gestionnaire. Ce sont des instruments très efficaces pour analyser les principaux risques pesant leur action.

Ce travail est suivi d'effets. Les ministères commencent maintenant à dépasser la stricte sphère du contrôle interne comptable, avec le développement d'un contrôle interne budgétaire et même, dans certains cas, de cartes des risques métier. Cela démontre une appropriation progressive de la démarche par les gestionnaires publics, au-delà des seuls comptables.

La certification des comptes sociaux apporte aussi une contribution majeure à la qualité et à la transparence de comptes publics de notre pays dont ils sont une composante essentielle. La meilleure fiabilité des procédures, la correcte application des décisions du législateur et de l'autorité règlementaire, le développement du contrôle interne sont des vecteurs d'efficience accrue, comme la Cour le constate année après année. Le régime général réalise chaque année des centaines de millions d'opérations. Compte tenu de ce volume énorme, la Cour cherche tout particulièrement à apprécier dans quelle mesure les systèmes d'information et les dispositifs de contrôle interne, par leur conception et leur mise en œuvre, permettent de maîtriser les risques d'anomalies ayant une incidence sur les comptes.

Le groupe « services publics » de l'association des directeurs financiers et de contrôle de gestion ne s'y est pas trompé, en consacrant une publication spécifique au dispositif de maîtrise des risques et de contrôle interne, au sein des organismes publics. Complément bienvenu au livre blanc sur la gestion des risques et le contrôle interne dans les collectivités territoriales, il propose aux gestionnaires publics des rappels utiles de méthodologie et d'organisation, tout en présentant des retours d'expérience, propres à illustrer concrètement la pratique du contrôle interne.

Il s'intéresse, à juste titre, à la maîtrise des risques et au contrôle interne dans tous les organismes publics. Les juridictions financières sont attentives, en effet, à ce que les meilleures pratiques de gestion soient diffusées dans toutes les administrations publiques. Par leurs contrôles et leurs évaluations, elles s'efforcent de les mettre en valeur. Mais le levier de la certification des comptes n'est pas encore généralisé. C'est pourquoi la Cour a appelé de ses vœux une expérimentation de la certification pour certaines collectivités territoriales. Elle devrait avoir pour conséquence une attention accrue du certificateur, quel qu'il soit, au contrôle interne.

En tout état de cause, l'approche par la comptabilité n'est qu'une première étape. La maîtrise des risques de gestion s'appuie certes sur le contrôle interne comptable, qui fournit des outils (carte des processus, carte des risques, plans d'actions, outils de reporting du contrôle interne), mais les risques financiers dépassent la sphère comptable. La clé réside certainement dans l'engagement des plus hautes autorités hiérarchiques des organismes, ce qui suppose de bien intégrer le contrôle interne dans les préoccupations de la gouvernance.

L'ouvrage de l'association des directeurs financiers et de contrôle de gestion pourra les guider vers une telle l'approche.

Le sujet est à n'en pas douter porteur pour le secteur public !

SOMMAIRE

SOMMAIRE

Remarque préliminaire :
Les avis et prises de position exprimés dans ce Livre Blanc sont le reflet des idées de leurs auteurs et n'engagent en aucune manière les institutions, organismes et collectivités dont ils font partie.

INTRODUCTION

Le Contrôle interne est-il une invention récente issue du monde financier des entreprises, qu'il s'agirait de propager au sein d'administrations, d'entreprises publiques ou de collectivités territoriales en mal de maitrise budgétaire ?

Ce point de vue, s'il ne s'exprime pas directement, est néanmoins diffus parmi les médias, et l'opinion publique pourrait facilement s'en persuader, en particulier à l'occasion du rite annuel de la publication du rapport de la Cour des Comptes. Les cas épinglés par les Magistrats de la Cour, montrent à l'évidence, dans de nombreuses situations, une absence de contrôle au sein d'entités publiques, soit par des gouvernances incapables de piloter leurs services, soit par des prises de décisions malencontreuses dont les effets désastreux se déploient inexorablement, sans réaction vigoureuse des dites gouvernances. Nous laissons de côté ici, les cas de malversations de fonds publics par des fonctionnaires ou des élus, qui sont heureusement rares dans notre pays, et pour lesquels globalement les contrôles traditionnels semblent efficaces.

L'entreprise privée rencontre elle des difficultés de même nature ?
Périodiquement des scandales apparaissent, soit par l'incompétence de certains dirigeants, soit par des pratiques illégales qui souvent d'ailleurs s'appuient sur des comptabilités erronées, voire truquées. Les pouvoirs publics de différents pays, dont au premier chef les USA, ont impulsés la mise en place de législations encadrant les pratiques managériales des dirigeants de sociétés faisant appel à des investisseurs, afin de les protéger des dérives constatées. La loi SOX [1] aux USA, la LSF [2] en France en sont des exemples qui se sont largement diffusés dans la plupart des pays développés. Ces lois qui visent à responsabiliser, y compris pénalement, les dirigeants des sociétés, s'appuient explicitement sur la qualité du contrôle interne qui doit être une préoccupation prioritaire du management. Pour donner un contenu concret à ces pratiques, les organismes (comme l'AMF[3] en France), chargés de la régulation de ces sociétés qui sont en général cotées sur des bourses de valeur, promeuvent un référentiel, le COSO [4], élaboré depuis maintenant plus de 20 ans et qui en est à sa quatrième version publiée en 2013.

Aux mêmes maux les mêmes remèdes ?
Dans cette perspective, le Contrôle interne deviendrait l'outil managérial commun à toutes les organisations dont la taille et la diversité des composantes en feraient des proies faciles pour les porteurs d'intérêts particuliers, voire individuels, au détriment de l'intérêt commun de l'organisation et des missions assignées par la gouvernance de l'entité. La distinction sphère publique / entreprise privée ne se manifesterait que par le mode de composition de la gouvernance (représentée par le conseil d'administration, émanation des actionnaires dans l'entreprise privée ou par la tutelle dans la sphère publique, qui en dernier lieu, exprime la volonté du citoyen et de ses représentants élus).

Sans plaider explicitement pour cette convergence des contrôles internes, le législateur français a mis en marche une série de mécanismes qui y conduisent. La LOLF[5] en premier lieu et la certification des comptes de l'Etat qui en découle logiquement[6], puis la réforme constitutionnelle de 2008 qui est venue élargir ce périmètre, en imposant cette exigence de qualité comptable à l'ensemble des comptes des administrations publiques constituées de l'Etat, du secteur public local et hospitalier et des autres établissements et organismes publics majoritairement financés sur des fonds publics en prescrivant que **« 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 ».**

Comme pour les entités privées, la qualité des comptes publics découle donc directement de la qualité du contrôle interne. La Cour des Comptes ne s'y trompe pas, puisque depuis sa première certification des comptes de l'Etat qu'elle assortit de réserves, les défauts de qualité du contrôle interne sont épinglés chaque année. Pour être plus précis notons que la Cour des comptes associe dans ces réserves aussi bien le contrôle interne que son audit interne[7].

Mais la complexité du monde public conduit ses acteurs à introduire une distinction dans leurs contrôles en précisant que le contrôle interne que nous venons d'évoquer n'est que le « contrôle interne comptable », auquel il faut adjoindre le « contrôle interne budgétaire » pour être complet.

Ce dernier aspect n'est certes pas à négliger, lorsque la maitrise des dépenses (et des recettes !) publiques devient un impératif catégorique pour un Etat confronté à un niveau d'endettement qui ne cesse de croitre. Mais n'est-ce pas introduire une faille dans le (ou les ?) contrôle(s) interne(s) ? Est-il possible d'exécuter correctement un budget (CI budgétaire validé) avec une médiocre qualité comptable (amortissements et provisions incohérents, par exemple) ? Beaucoup d'observateurs le redoutent et demandent la mise en place de coopérations beaucoup plus fortes entre ordonnateurs et comptables publics.

Ainsi, dans cette perspective, il va s'agir de « recycler » ou de mettre en cohérence des pratiques existantes de contrôles au sein de la sphère publique, pour les aligner sur de nouvelles approches transposées des normes en vigueur dans les entreprises privées.

La boite à outils des « contrôleurs privés » est-elle plus performante que celle des « contrôleurs publics » ?

(1) *« loi Sarbanes-Oxley », du nom de ses promoteurs : le sénateur Paul Sarbanes et le député Mike Oxley, votée en 2002.*

(2) *La Loi de sécurité financière, votée en 2003.*

(3) *L'Autorité des marchés financiers (AMF) est une autorité publique française indépendante créée en 2003 qui a en charge la régulation des marchés financiers et la protection de l'épargne investie.*

(4) *COSO est l'acronyme abrégé de Committee Of Sponsoring Organizations of the Treadway Commission, une commission à but non lucratif qui établit en 1992, aux USA, une définition standard du contrôle interne, ce référentiel est désormais repris internationalement.*

(5) *La loi organique relative aux lois de finances (abrégée en LOLF) est le texte déterminant le cadre juridique des lois de finances. Votée en 2001, elle s'applique désormais à toutes les administrations publiques.*

(6) *La certification de la régularité, de la sincérité et de la fidélité des comptes de l'Etat, prévue par le 5° de l'article 58 de la LOLF a été publiée pour la première fois à partir des comptes de l'année 2006.*

(7) *Réserves formulées sur les comptes de 2013 : « réserve n° 2 : les dispositifs ministériels de contrôle interne et d'audit interne sont encore trop peu effectifs et efficaces ; ». Il est à noter que cette réserve est récurrente depuis 2006.*

La méthodologie du dispositif de Contrôle Interne

1

1. LES FONDEMENTS DE LA DÉMARCHE DE MAÎTRISE DES RISQUES ET DE CONTRÔLE INTERNE

Le dispositif de Contrôle Interne (DCI – appelé également Système de Contrôle Interne ou SCI1) est un système de management intégré, s'appuyant sur deux composantes essentielles que sont la Gestion des Risques et le Contrôle Interne, définies au sens du référentiel COSO. Le contrôle interne fait donc partie d'une démarche qui doit être globale, systémique et systématique.
Son but est de « fournir une assurance raisonnable » quant à la réalisation d'objectifs entrant dans les catégories suivantes :

- « La réalisation et l'optimisation des opérations dans le respect des engagements de service et de l'intérêt général » ;
- « La fiabilité des informations financières » ;
- « La conformité aux lois et aux réglementations en vigueur ».

Ces trois catégories d'objectifs ont été définies dans le COSO (acronyme signifiant Committee Of Sponsoring Organizations of the Treadway Commission), transposé en France par l'Autorité des Marchés Financiers (AMF), pour ce qui concerne le secteur privé. Le modèle COSO est la référence, volontaire ou obligatoire (elle est reprise par la Cour des comptes), de la mise en place du Contrôle Interne au sein d'une structure. Elle permet d'évaluer la maturité du système de Contrôle Interne (SCI).

D'autres catégories de risques peuvent être ajoutées afin de compléter les objectifs auxquels doit répondre une démarche de Contrôle Interne dans cet environnement spécifique :

- La prévention et la détection des erreurs et des fraudes ;
- La protection des ressources et du patrimoine ;
- La sécurité des personnes accueillies au sein d'une structure publique.

Un Contrôle Interne efficace implique la nécessité d'identifier les risques et de mettre en place les actions qui permettent de maîtriser ces risques. Une démarche de gestion de risques intégrée au dispositif de Contrôle Interne est donc indispensable afin de renforcer le Contrôle Interne d'une organisation.

1.1. Les principes de la démarche de maîtrise des risques et les apports du COSO 3

La maîtrise des risques est généralement définie comme étant une étape de la démarche globale de Contrôle Interne. Il s'agit d'une démarche complémentaire à celle du Contrôle Interne ayant un même objectif : sécuriser les processus de la structure concernée afin de l'accompagner dans la réalisation de ses objectifs et de l'aider à tenir ses engagements. Elle est définie dans le COSO comme étant « l'identification, l'évaluation et le choix du traitement des risques ».

Le COSO 2 complète le référentiel de Contrôle Interne COSO en proposant un cadre de référence pour la gestion des risques. Il définit la gestion des risques comme un processus transversal à une organisation qui contribue à l'élaboration et à la mise en œuvre de sa stratégie globale tout en permettant d'identifier les évènements potentiels pouvant l'affecter. Mettre en place une solution pour maîtriser ces risques implique donc de fixer des limites d'appétence au risque (la notion de « risk appetite ») et de faire en sorte que les risques soit maintenus en deçà des limites fixées.
Une nouvelle version du référentiel COSO a vu le jour en 2013. Intitulé COSO 3, il remet au goût du jour le cadre de référence du Contrôle Interne en intégrant les principaux changements survenus ces dernières années en termes de méthodologie et de trajectoire. Il s'agit, en premier lieu, d'identifier les risques nouveaux et d'adapter les dispositifs pour mieux répondre aux évolutions de l'environnement ; en second lieu, de renforcer les dispositifs de Contrôle Interne et de gestion des risques en prenant mieux en compte les composantes internes et externes de l'entreprise/l'organisme (les ressources, la technologie, les opérations, etc.) et en développant les outils que sont le reporting et la conformité.
Les nouveautés apportées par le COSO 3 sont abordées de façon plus détaillée en annexe.
Ainsi, afin de prendre en compte les cadres de référence et les récentes évolutions, la démarche de gestion des risques s'articule en quatre grandes étapes distinctes, précédée d'une phase de pré-requis :

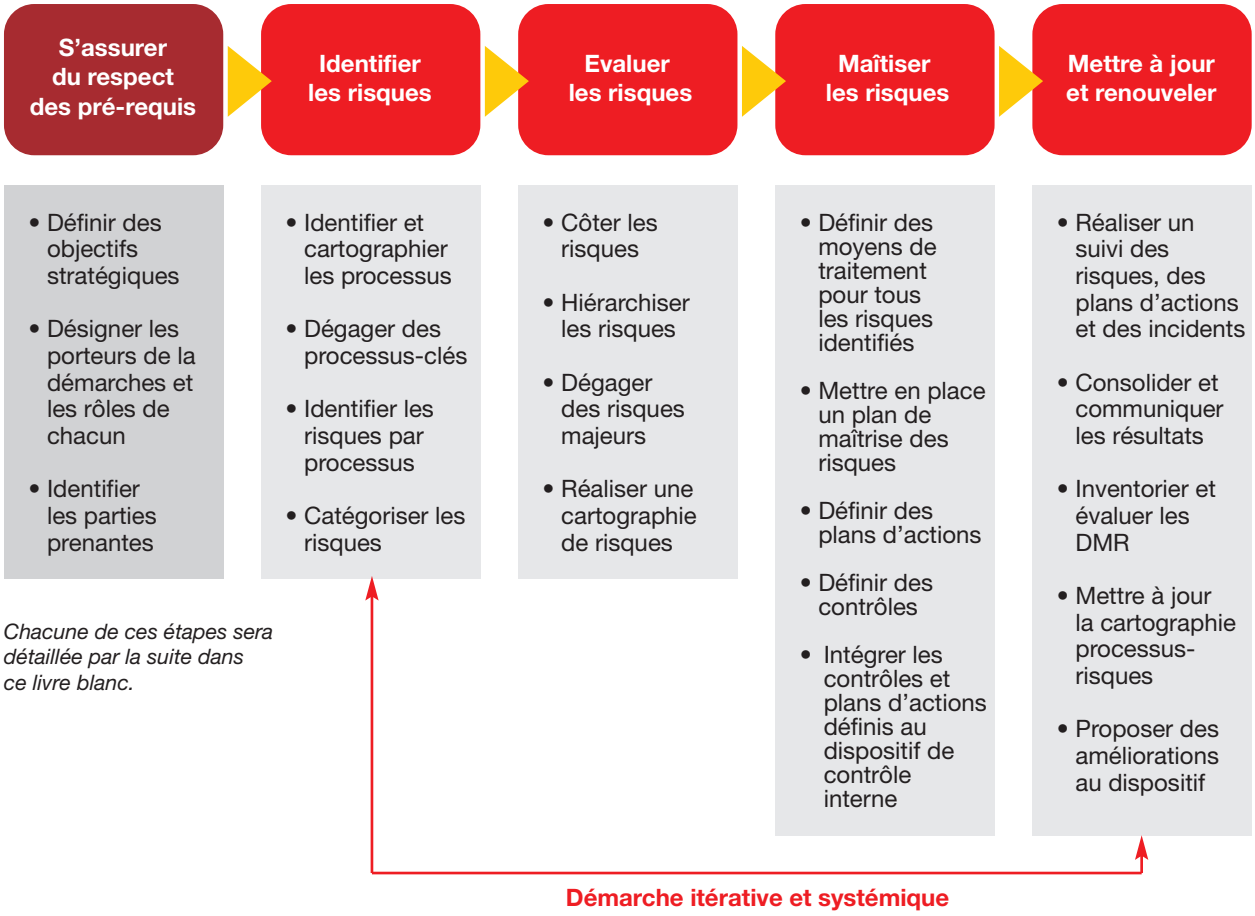
- L'étape préliminaire de pré-requis – définition des objectifs de la démarche, désignation des porteurs et des acteurs de la démarches et identification des parties prenantes ;

(8) SCI ou DCI seront utilisés indifféremment dans ce présent Livre Blanc

- L'identification des risques – identification et cartographie des processus, identification des risques pour chaque processus ;
- L'évaluation des risques – évaluation et cotation des risques ; obtention d'une cartographie des risques ;
- La maîtrise des risques – définition des moyens de traitement des risques ; mise en place de dispositifs de maîtrise des risques (DMR) ; élaboration de plan d'actions ;
- Le suivi et la mise à jour de la démarche - inventaire, suivi et évaluation des dispositifs de maîtrise des risques (DMR) ; suivi des plans d'actions ; gestion des incidents ; reporting ; mise à jour de la cartographie des risques.

La dernière étape est fondamentale, elle permet de mesurer l'efficacité de la démarche de gestion des risques mais également de l'améliorer afin de mettre en place un dispositif résilient et adaptable aux évolutions futures de l'organisation.

Le schéma suivant présente un modèle général de démarche de gestion des risques pour le secteur public, rassemblant les cinq grands axes :



Chacune de ces étapes sera détaillée par la suite dans ce livre blanc.

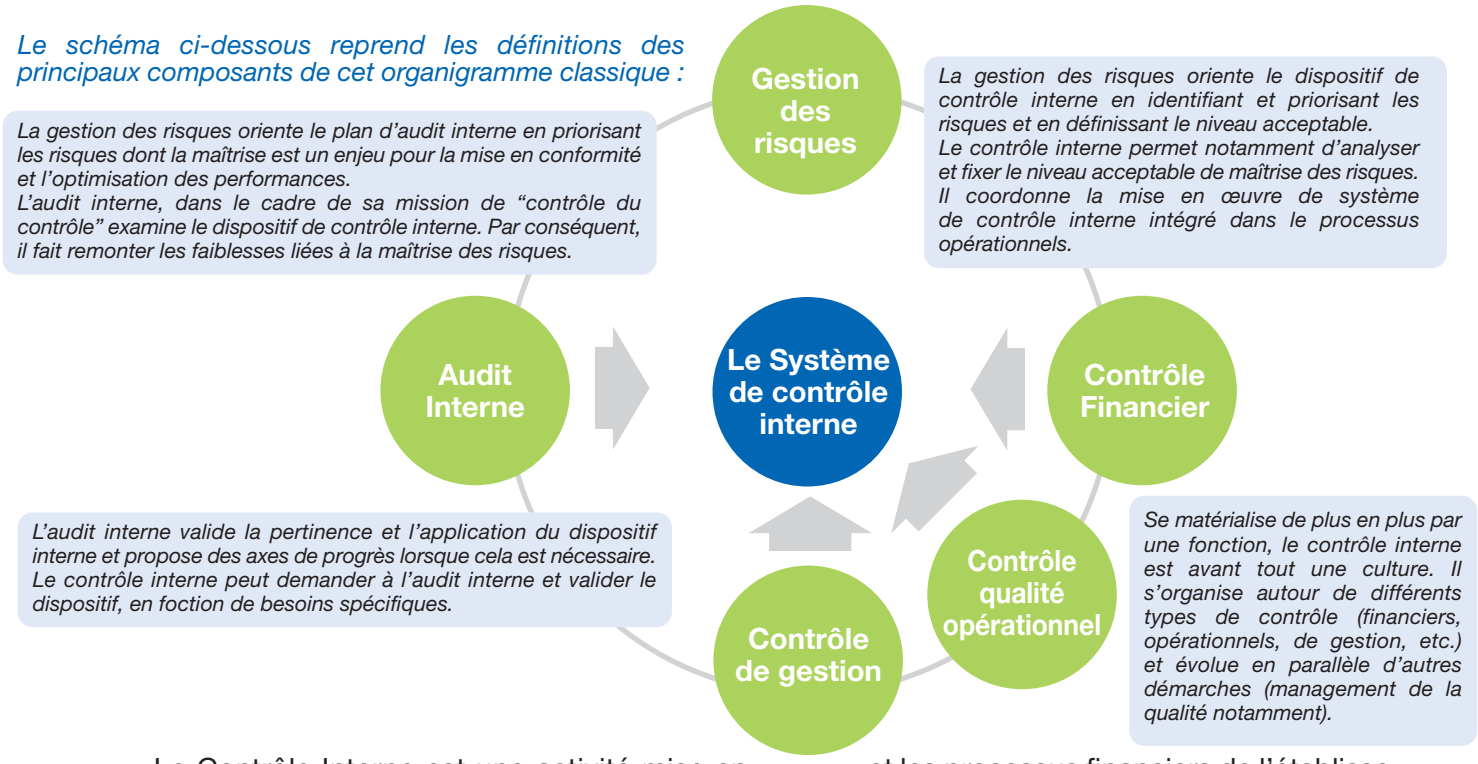
1.2. La gouvernance

1.2.1. L'articulation entre Contrôle Interne, gestion des risques, audit et suivi opérationnel

La démarche de gestion des risques doit être mise en relation avec les autres systèmes de contrôles au sein d'une organisation. Si l'"organigramme" classique - et théorique - d'un système de Contrôle Interne au sein d'une entreprise, nécessite d'être adapté aux organisations du secteur public, il est toutefois opportun de rappeler la répartition habituellement rencontrée des rôles entre les trois principales fonctions que sont la gestion des risques, l'audit interne et le Contrôle Interne.

Un système global de Contrôle Interne, ayant atteint un certain degré de maturité, intègre donc en plus de la démarche de gestion des risques, les démarches d'audit interne, et les processus de contrôle liés aux activités de l'organisation : contrôle financier, contrôle de gestion, contrôle qualité opérationnel.

Le schéma ci-dessous reprend les définitions des principaux composants de cet organigramme classique :



Le Contrôle Interne est une activité mise en oeuvre par la direction d'une organisation dans le but de vérifier la mise sous contrôle et la sécurisation de ses processus. Il vérifie que les actions de maîtrise des risques sont pertinentes et correctement mises en place. Son objectif est de mettre en place des dispositifs de maîtrise qui permettront de donner à la Direction Générale l'assurance raisonnable que les risques de l'organisation sont bien maîtrisés, notamment par l'intermédiaire des remontées conséquentes liées aux missions d'audit.
La maturité du système de Contrôle Interne se mesure également au degré de sensibilisation des agents opérationnels à la démarche de gestion des risques ainsi qu'à la qualité de la documentation produite. Pour cette raison, le Contrôle Interne semble devenir progressivement une véritable fonction des organisations matures, au même titre que les ressources humaines, les finances, etc. Elle est dans ce cadre souvent associée à une direction fonctionnelle correspondante. Outre son rôle formateur, de synergie et de centralisation, cette direction est notamment responsable in fine du système de Contrôle Interne déployé au sein de l'organisation.

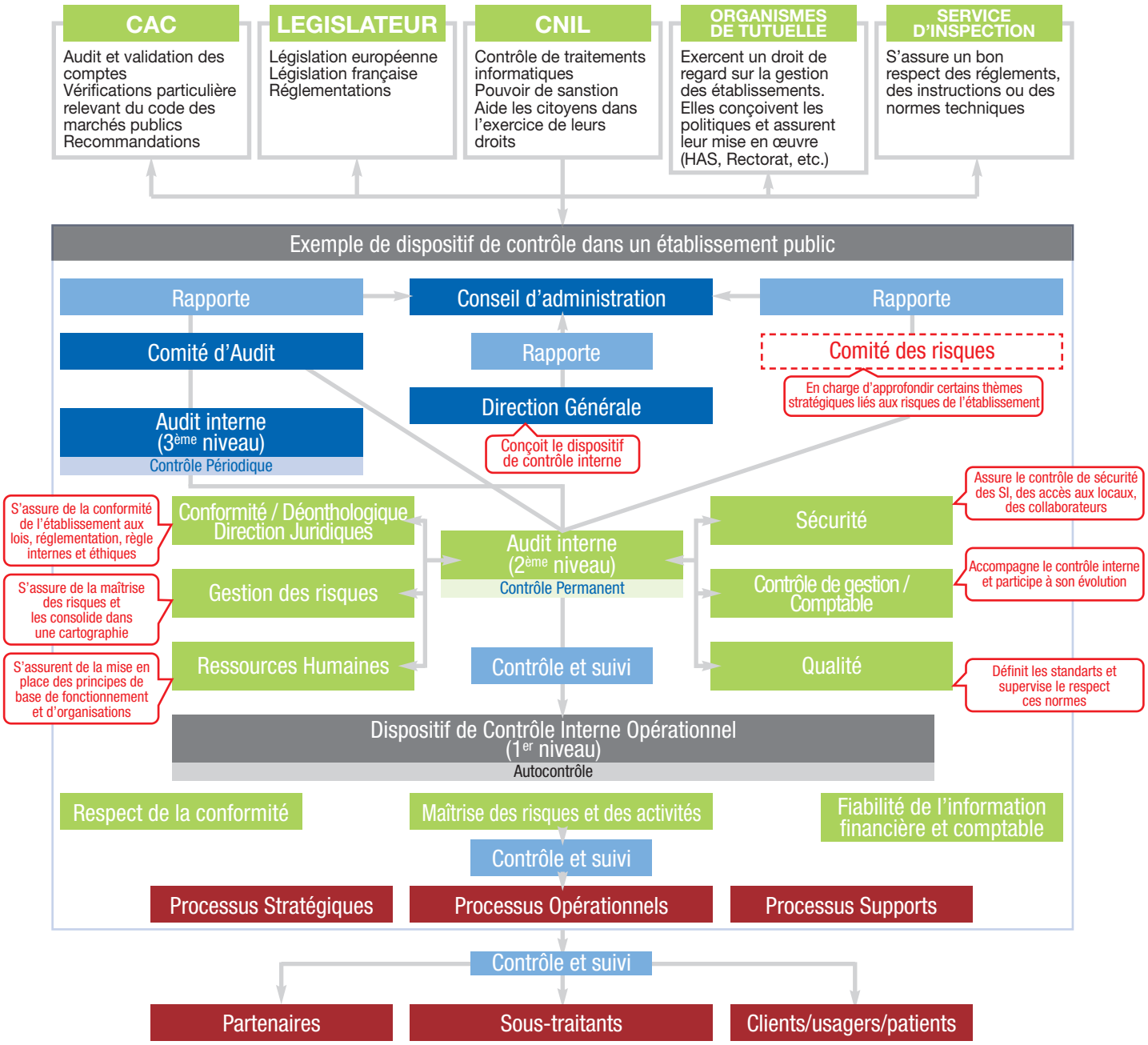
Concernant la démarche de gestion des risques plus spécifiquement, plusieurs directions ou départements sont en charge de réaliser des contrôles liés aux activités de l'établissement. Ces directions sont souvent les premières à mettre en place des démarches internes intégrant la gestion des risques :

- Par exemple, les directions financières, en charge des processus de contrôle financier, et le contrôle de gestion opèrent un premier niveau de contrôle sur les flux et les processus financiers de l'établissement ;
- Le département Qualité joue également un rôle conséquent dans la démarche de maîtrise des risques car celui-ci est en charge de réaliser des contrôles sur les processus opérationnels. Le département de la Qualité a effectivement en place un certain nombre de contrôles afin d'assurer la qualité des produits fournis par l'établissement. Il définit en amont des objectifs de qualité, de performance et de rendement, et s'assure ensuite que ceux-ci ont été atteints. La démarche ainsi mise en oeuvre permet donc de couvrir un certain nombre de risques, tels que les risques de défaillances du fonctionnement d'un processus opérationnel de l'établissement ; de défaillances des fournisseurs/sous-traitants/délégataires ; ou encore d'insatisfaction des bénéficiaires. La démarche de qualité réalisée par la Direction de la qualité est une démarche complémentaire à la démarche de maîtrise des risques, qui vient compléter le dispositif de Contrôle Interne d'un établissement public.

1.2.2. La répartition des rôles et des fonctions / La définition des différentes responsabilités des acteurs du Contrôle Interne pour la mise en place de la démarche

Cette présentation vise à identifier de la manière la plus exhaustive possible l'ensemble des organes et composantes d'une gouvernance de gestion des risques et de Contrôle Interne.

Cet exemple ne prétend pas être la seule gouvernance possible et il convient de l'adapter en fonction des spécificités des organismes publics (taille, forme juridique, organisme de tutelle, etc.) et au regard des moyens humains à disposition.



Définir les responsables de la démarche de maîtrise des risques

Il est important de pouvoir s'appuyer sur une gouvernance forte lors de la mise en place d'une démarche de Contrôle Interne et donc de gestion des risques. S'agissant d'un processus transverse ayant un impact sur plusieurs directions ou départements à la fois, la démarche sera d'autant plus efficace et facile à mettre en place si un sponsor influent au sein de l'établissement appuie la démarche. L'appui de la Direction Générale est essentiel.
Le soutien du sponsor permettra en effet de légitimer les actions des personnes en charge de la mise en place d'une démarche de gestion des risques.

Cette démarche nécessite ensuite la désignation d'un responsable ou pilote. Suivant la maturité du système de Contrôle Interne en place au sein de l'établissement, il sera plus ou moins évident de désigner les responsables de la démarche. Au sein d'un dispositif mature, formalisé et organisé, un Responsable risques ou une Direction des risques sera peut-être déjà en place. Celui ou celle-ci sera donc en charge de la mise en place de la démarche des risques. Au sein d'un établissement moins mature en termes de gestion des risques, il sera peut-être plus difficile d'identifier une personne à même de porter cette démarche. La démarche de gestion des risques étant très liée à celle de Contrôle Interne, il sera donc logique que le pilote de la démarche de gestion des risques soit une personne issue du Contrôle Interne.

Nonobstant cela, l'implication de sponsor(s) et d'un pilote est nécessaire à la mise en place d'une démarche de gestion des risques au sein d'un établissement. Une fois ces personnes clairement identifiées, il restera au responsable à identifier les acteurs ainsi que les parties prenantes au

dispositif de gestion des risques. La connaissance de toutes les parties impliquées dans le processus facilite au même titre que l'influence d'un sponsor les actions de mise en place, de communication ou de coordination qui seront prises dans le cadre de la mise en place d'une démarche de maîtrise des risques au sein d'un établissement public.

Le Conseil d'Administration

Selon l'article 225-35 du Code du Commerce, le Conseil d'Administration « oriente les activités de la société et veille à leur mise en oeuvre ». Il doit également « se saisir de toute question intéressant la bonne marche de la société et règle par ses délibérations les affaires qui la concernent ». Enfin, il est « tenu de procéder aux vérifications et contrôles qu'il juge opportun ».

Dans le cadre du Contrôle Interne, ces dispositions font notamment intervenir le Conseil d'Administration sur la définition de la stratégie. Notamment, la question de l'appétence aux risques, telle que définie par le référentiel COSO, est centrale : quel niveau de risque l'organisation est-elle prête à accepter ?

Le Conseil d'Administration est responsable de l'application de cette orientation, ce qui implique un rôle de supervision de l'organisation notamment par le biais du Comité d'Audit.

Les missions du Conseil d'Administration sont dans ce domaine sont multiples. Il doit :

- S'assurer de l'existence dans l'organisation des composantes nécessaires au Contrôle Interne (ressources, procédures…) ;
- Inclure la gestion des risques dans les processus de décision stratégique ;
- Garantir la fiabilité de l'information communiquée aux actionnaires en intégrant convenablement la donnée des risques ;

Le Conseil d'Administration est engagé envers les actionnaires, la société et les tiers. Avec la crise financière de 2008, cette responsabilité tend à augmenter. Les administrateurs ne sont plus à l'abri de poursuites civiles dans le cas où ils auraient failli à remplir correctement leur mission d'orientation et surtout de supervision.

Le Comité d'Audit

Dans le cadre de sa mission de surveillance, le Conseil d'Administration délègue au Comité d'Audit la charge de garantir pour lui la qualité du Contrôle Interne et la fiabilité de l'information donnée aux actionnaires. Il conserve toutefois la responsabilité en dernier ressort de cette supervision. Les membres du Comité d'audit sont issus du Conseil d'Administration dont ils sont, aux deux-tiers des membres indépendants.

Dans la pratique, l'influence du Conseil d'Administration sur le Contrôle Interne pratiqué par le management de l'organisation s'effectue principalement par le biais du omité d'Audit. Ce dernier est en effet plus à même d'apprécier les enjeux de ces questions, grâce à ses liens avec l'audit interne. Il entend régulièrement les responsables de ce dernier, et donne son avis sur les problématiques soulevées.

Le Comité d'Audit est une obligation depuis la Loi de Sécurité Financière (LSF) de 2003 (« Loi Mer ») pour toutes les entreprises cotées. Sa présence renforce la qualité de la gouvernance mise en place au sein de l'organisation. Elle améliore l'image et la confiance des parties prenantes et des actionnaires.

Si la création d'un Comité des Risques distinct du Comité d' Audit n'est pas obligatoire, elle peut être dictée par la complexité des risques à superviser. Le Comité d'Audit conserve la supervision des risques de nature comptable et financière ; pour les autres risques, notamment pour les risques métiers, un partage des rôles doit être défini avec le Comité des Risques.

Le Comité des Risques a pour missions :

- D'identifier les risques majeurs auxquels l'organisation est confrontée,
- De s'assurer que les moyens de suivi et de maîtrise de ces risques ont été mis en place,
- De s'assurer de l'adéquation de la couverture des risques avec le niveau de risque résiduel
- D'analyser les risques assurables et le programme d'assurances
- Le suivi de plans d'actions sur des risques spécifiques
- D'examiner la politique d'Enterprise Risk Management

Concernant les administrations, l'obligation de mettre en place un comité d'audit a été fixée par le décret n°2011-775 du 28 juin 2011. Ce décret pose l'obligation de mise en oeuvre d'un dispositif de maîtrise des risques fondé sur le contrôle et l'audit interne dans chaque ministère. Ainsi, au sein de chaque administration un comité ministériel d'audit interne doit être créé. Garant de l'indépendance, du professionnalisme et de l'objectivité des auditeurs internes dans l'exercice de leurs missions d'assurance et de conseil, ce comité a pour mission de :

- Définir la politique d'audit de l'établissement public ;
- S'assurer de la qualité du dispositif de Contrôle Interne et de maîtrise des risques ;
- Approuver le programme des audits ministériels ;
- Assurer le suivi des actions décidées à l'issue de ces audits.

L'audit Interne
La fonction de l'audit interne rend compte au Comité d'Audit, pour lequel elle réalise les missions de contrôle périodique ou exceptionnel. La gestion des risques fait donc partie intégrante de son champ d'action, notamment dans l'évaluation de son efficacité au sein de l'organisation.

L'une des responsabilités de l'audit interne est d'évaluer l'acceptation des risques faite par le management en fonction du profil de risque de l'entreprise et de l'appétence de la Direction Générale. Si celle-ci ne correspond pas à l'orientation définie par le Conseil d'Administration, ce dernier doit en être informé par le Responsable de l'Audit
Interne.

Au quotidien, l'audit interne travaille en collaboration avec le management de l'organisation pour questionner leur gestion des risques et les processus concernés. Toutefois, il n'a pas vocation à assumer un rôle opérationnel dans ces processus.

La Direction Générale
La Direction Générale est l'organe de décision principale de la société. A ce titre, elle est responsable de la formulation stratégique des consignes d'appétence aux risques données par le Conseil d'Administration.
L'appétence aux risques reflète le niveau de risque acceptable pour la Direction Générale dans le cadre son processus de prise décision stratégique.

Son rôle est central à plus d'un titre. Tout d'abord, par la manière dont elle impacte la culture du risque dans l'organisation par son implication. Voir la Direction Générale jouer un rôle de « sponsor » peut ainsi faciliter considérablement l'intégration de la culture risque dans les processus métiers.

C'est elle qui conçoit le dispositif de Contrôle Interne de l'organisation, soit directement, soit par le biais d'une Direction des Risques dédiée. Dans ce cadre, l'organisation de ce système, la responsabilité des acteurs et leur rôle sera déterminant dans son bon fonctionnement. De même, il doit intégrer une composante liée à la bonne circulation de l'information entre tous les agents.

Dans tous les cas, elle est responsable devant le Conseil d'Administration de lui communiquer les risques stratégiques et les problématiques du Contrôle Interne.

La Direction du Contrôle Interne et de la Gestion des risques
La gestion des risques identifie et analyse les risques devant être maîtrisés par l'organisation. Elle demande la conception de plans d'actions et de contrôles permettant de répondre de façon efficace à ces risques. Le Contrôle Interne est responsable de la mise en oeuvre de ces contrôles ainsi que de celui du dispositif de gestion des risques.
Ces deux composantes sont donc complémentaires et ont vocation à être traitées au sein d'une même direction.
Les missions confiées à cette direction sont donc les suivantes :

- Appliquer les orientations et instructions confiées par la Direction Générale
- Assurer le bon fonctionnement des processus de l'organisation notamment ceux qui concourent à la sauvegarde de ses actifs
- Garantir la fiabilité des informations financières par une procédure de Contrôle Interne assurant la bonne prise en compte des opérations réalisées par l'organisation

La Direction du Contrôle Interne et de la Gestion des Risques est majoritairement placée sous l'autorité de la Direction Générale. Dans certains cas, la fonction de Contrôle Interne et la Gestion des Risques sera rattachée à la Direction financière, au Secrétariat Général, ou même à la Direction Juridique. Cependant le lien avec la Direction financière serait dans la mesure du possible à éviter en raison de "conflits d'intérêts" en lien avec le SCI financier (sous l'angle Sarbanes Oxley) d'une part, pour que le SCI se déploie aussi sur les activités non financières (SCI dit opérationnel) d'autre part.

La Direction de la conformité
La mise en conformité de l'organisation est une tâche pouvant être décomposée en deux parties :

- Un examen de la règlementation et des lois en vigueur pour analyse et adaptation à l'organisation ;

- L'implémentation et le contrôle de ces adaptations.

Or, ces deux tâches requièrent des compétences spécifiques. L'implémentation dans les processus et le contrôle en continu relèvent de la responsabilité du Contrôle Interne. Cependant, l'analyse de la règlementation et des lois en vigueur sont des travaux à valeur juridique.

La répartition des responsabilités entre Direction de la Conformité, Direction Juridique et Direction du Contrôle Interne doit ainsi être soigneusement étudiée en fonction de la taille de l'organisation et de l'importance des exigences règlementaires. Selon ce critère, le choix pourra être fait d'une Direction de la Conformité dédiée avec ses compétences propres ou bien la mise en place d'un « mode projet » pour la gestion règlementaire, transverse dans la gouvernance entre Direction Juridique et Contrôle Interne.

La Direction des Systèmes d'Informations
Les systèmes d'informations sont aujourd'hui omniprésents dans les organisations publiques. Leur importance est d'autant plus grande qu'ils permettent l'automatisation d'une grande partie des tâches du contrôle, en gérant par exemple les autorisations pour chaque membre opérationnel.
Cette direction, qui assure la maintenance, la conception, la recherche des systèmes d'informations n'a donc pas qu'un rôle technique. Elle doit en effet à la fois maitriser les risques pouvant être contrôlés par automatisation mais également travailler en collaboration avec la Direction du Contrôle Interne pour garantir ceux ayant besoin d'une couverture additionnelle.

La Direction des ressources humaines
Les ressources humaines ont une importance réelle dans la gouvernance du risque par leur rôle de formation. En amont même du recrutement, l'objectif d'insérer dans l'entreprise une « culture du risque » nécessite de vérifier que les candidats y seront réceptifs et, le cas échéant, formés.
La définition d'une politique du personnel en accord avec cet objectif est donc une priorité forte d'un Contrôle Interne efficace, facilitant le travail en aval de la direction des risques.

Les directions métiers
Les Directions métiers sont au coeur de l'activité et donc de la nécessité de la mise en oeuvre d'une gestion des risques efficace. Avant l'intervention de la Direction du Contrôle Interne, elles sont en première ligne de la maîtrise des procédures et nécessités de contrôle. Etant expertes dans leur métier respectif, elles ont également pour responsabilité de participer à la construction des systèmes de contrôle avec la Direction du Contrôle Interne.
Elles devront également tenir à jour leur cartographie des risques, dans l'optique d'un contrôle permanent permettant une remontée efficace de l'information.

Les opérationnels
L'application des procédures de Contrôle Interne est tributaire de l'implication des opérationnels. Ces derniers sont en effet les contributeurs principaux d'un tel système, et en assurent la pérennité par un premier niveau dit « d'autocontrôle ».

Le rôle de la « culture du risque », telle que promue par la Direction Générale et les ressources humaines, est déterminant. C'est elle qui permettra aux agents opérationnels d'agir dans une démarche intégrant la problématique de risque dans le cadre des bornes délimitées par l'organisation. C'est elle qui permettra aux agents opérationnels d'intégrer la problématique de risques dans la réalisation de leurs tâches quotidiennes.

La Direction du Contrôle de gestion
Le Contrôle de Gestion possède une connotation plus financière que le Contrôle Interne. Son importance doit être soulignée dans les organisations publiques : il permet en effet d'assurer une meilleure cohérence et performance financière, mais également de transmettre des données de risque financier à la Direction du Contrôle Interne.

Ses outils, rodés à l'évaluation de la performance, possèdent une bonne compatibilité avec ceux du Contrôle Interne.

Le Direction du Contrôle qualité
Le Contrôle Qualité, habitué au travail sur les processus par la nature de son travail, est un allié précieux du Contrôle Interne dans l'entreprise. Ayant pour mission de garantir la qualité des biens et des services destinés aux usagers, il doit s'assurer que les procédures internes et les normes sont connues et appliquées correctement.

Dans ce cadre, le Contrôle Interne peut s'appuyer sur le Contrôle Qualité pour obtenir des retours fiables sur d'éventuels risques touchant aux prestations fournies. La sensibilisation de cette direction à la « culture

du risque » peut donc aider à garantir une « assurance raisonnable » aux dirigeants.

Les organismes externes : filiales et sous-traitants

Avec la tendance toujours plus forte au « sourcing » des agents économiques et à l'internationalisation des firmes, il est devenu vital pour l'organisation de pouvoir contrôler le risque inhérent à ses sous-traitants et filiales.

Les cas des filiales et sous-traitants sont certes différents mais ont pour origine la même problématique : comment soumettre au Contrôle Interne des éléments externes à l'organisation ?

Le contrat liant l'organisation à son prestataire doit donc inclure cette problématique par le biais d'exigences sur lereporting et l'audit externe. L'expertise de la Direction des achats, rodée à la sélection de fournisseurs sur des critères précis de qualité, de prix, mais également de solidité financière par exemple, peut ici être précieuse à l'organisation. La planification d'une mission transverse Achats/Contrôle Interne, toujours chapeautée par la Direction Générale, doit ainsi être envisagée lorsque le risque sous-traitant dépasse le seuil négligeable.

Enfin, le problème des filiales relève de la difficulté de faire coïncider des systèmes de Contrôle Interne parfois très différents, tant dans leur organisation que dans leur profondeur. Pour autant, le risque « filiale » n'est pas à négliger.

Le statut de filiale n'épargne donc pas à la société-mère les vérifications qu'elle ferait pour une entité interne à l'organisation en matière de Contrôle Interne. Elle est responsable, solidaire et partie prenante des risques qui peuvent affecter cette entité externe. Elle doit donc agir en conséquence en matière de risques.

Les particularités des EPA (Etablissements Publics Administratifs) et de l'Administration Publique

Les sociétés publiques (société de droit commercial dont l'Etat est un actionnaire majoritaire) et les EPIC (Etablissements Publics à Caractère Industriel et Commercial) ne disposent pas, dans la gouvernance du Contrôle Interne et de la gestion des risques, de grandes différences avec les sociétés de droit privé. Elles ont en effet les mêmes problématiques, à la différence qu'elles ont un engagement non pas envers des actionnaires privés mais envers l'Etat. L'une des conséquences est que ce sont les comptables publics qui se chargent de la comptabilisation des opérations. Mais en définitive, ces organisations disposent d'une responsabilité propre sur leurs politiques de Contrôle Interne et de gestion des risques et leur gouvernance en la matière est donc comparable à celle des sociétés privées présentées préalablement.

En revanche, les EPA (Etablissements Publics Administratifs) et Directions ministérielles, sont des organisations dépendant directement des Ministères. Dans ce cadre, le fonctionnement du Contrôle Interne est radicalement différent, puisqu'il est sous tutelle du Comité d'Harmonisation de l'Audit Interne (CHAI), définissant un cadre de référence ensuite adapté par chaque Mission Ministérielle d'Audit Interne (MMAI) et chaque Comité Ministériel d'Audit Interne (CMAI). Ce sont ces entités qui se chargent également de la définition du Contrôle Interne et de la gestion des risques pour les organisations sous la tutelle de leur ministère respectif.
En supplément de cette supervision, la hiérarchie directe, les inspections générales et les contrôles effectués par les comptables publics sont en général les principaux intervenants du Contrôle Interne. Ainsi, si l'on peut identifier les organes décideurs de la stratégie en matière de risque relativement facilement, il existe un flou dans l'attribution opérationnelle de la gestion des risques et du Contrôle Interne : certaines directions ont pu développer leur propre système de Contrôle Interne tandis que d'autres dépendent encore exclusivement des inspections générales ou des recommandations de la MMAI.

Les collectivités locales telles que les régions disposent également d'une organisation différente, dépendant de leurs compétences respectives et de leurs projets. Si elles se sont progressivement appropriées les problématiques de Contrôle Interne et de gestion des risques, elles élaborent encore au cas par cas la répartition des responsabilités sans cadre commun. Leur fonctionnement « Projet » dans le cadre des attributions de marchés publics nécessite un Contrôle Interne rigoureux pour répondre aux exigences de coût et de qualité des contribuables.

La définition de la gouvernance est donc une problématique clé de la gestion du risque et du Contrôle Interne des organisations publiques.

La séparation des tâches : gouvernance, contrôle, opérationnel
La séparation des tâches dans la gestion des risques est une problématique-clé de son bon fonctionnement.

La séparation des tâches est un des principes fondateurs de la démarche de Contrôle Interne. Dans un souci de transparence et pour se prémunir du risque de fraude, il est impératif que l'organisation, quelque soient la taille ou la catégorie de secteur public applique ce principe. D'un point de vue structurel, cela se concrétise par la séparation des fonctions entre celui qui prend la décision, celui qui l'exécute et celui qui contrôle que cette décision a bien été exécutée. D'un point de vue plus opérationnel, par exemple, cela se traduit par une séparation des tâches entre la personne qui est en charge de la préparation du chèque de la personne qui les signe et de la personne qui va s'assurer que le chèque a bien été émis.

Responsabilité civile & pénale des organisations publiques
La répartition des rôles et la définition d'une gouvernance claire nécessitent également d'établir clairement les responsabilités. En effet, dans le privé, les administrateurs sont de plus en plus exposés à des poursuites pénales, avec un renforcement du nombre de procédures.

Dans les organisations publiques, des infractions sur les règles d'hygiènes et de sécurité peuvent notamment mener à une mise en cause des responsabilités pénales de l'autorité des collectivités. Cela inclut le maire, le président du conseil général, le président du conseil régional, le président, selon l'organisation impliquée.

L'usage des délégations de pouvoirs, indispensables au bon fonctionnement des administrations, peut ici jouer un rôle protecteur en déchargeant les responsabilités au niveau hiérarchique correspondant. La bonne gestion de ces délégations, considérée comme un point critique de la gestion des risques juridiques ces dernières années, est donc un élément particulièrement important à prendre en compte dans la conception du Contrôle Interne.

Il est donc essentiel de garder à l'esprit que les élus ne sont pas à l'abri d'une mise en cause personnelle, ce qui nécessite une vigilance constante vis-à-vis du risque juridique en particulier.

FOCUS SUR : Le décret 2011-775 du 28 Juin 2011
A l'origine, la fonction d'audit interne est ministérielle. Chaque Ministère gère indépendamment la supervision de ses opérations. Cependant, l'évolution de la règlementation dans le privé et la nécessaire optimisation des performances dans les organisations publiques ont imposé une structuration de cette fonction au plus haut niveau de décision.

C'est pourquoi le Premier Ministre promulgue en Juin 2011 le décret 2011-775 qui permet la création de trois entités au sein de l'administration française :

- Le Comité pour l'Harmonisation de l'Audit Interne (CHAI), de niveau interministériel, rassemble des représentants des missions d'audit de chaque ministère afin d'établir un cadre commun de référence et d'échanger les « best practices » (bonnes pratiques).
- Les Comités Ministériels d'Audit Interne (CMAI), chargés de définir les politiques ministérielles d'audit interne et de superviser les Missions Ministérielles d'Audit Interne (MMAI), notamment en approuvant leur programme d'audit.
- Les Missions Ministérielles d'Audit Interne (MMAI), chargées de programmer les audits au sein du Ministère et de diffuser en son sein les bonnes pratiques.

Le choix d'une structure « décentralisée », par ministère, est à l'origine du besoin d'une instance interministérielle capable de fonder le cadre de référence.

1.3. L'approche par la maîtrise des risques
Les menaces qui pèsent sur l'organisation sont permanentes et nombreuses et trouvent leur source au sein de l'environnement interne et externe de l'entreprise, mais aussi au travers des métiers, des processus opérationnels de l'établissement et des systèmes d'information. Afin de prendre les décisions adéquates faces à ces menaces, il est indispensable d'avoir une vision globale de ces risques et de les hiérarchiser pour pouvoir engager rapidement des actions préventives et de sécurisation. L'élaboration d'une cartographie des risques est l'outil de référence pour formaliser et hiérarchiser les risques majeurs et elle contribue par ailleurs à instaurer avec l'ensemble des collaborateurs de l'organisation un langage commun sur les risques.

La construction de la cartographie des risques peut être réalisée selon deux approches qui peuvent être utilisées indépendamment ou de manière combinatoire. La première approche consiste à réaliser une identification des risques par les services ou entités opérationnels pour permettre une remontée des risques au plus prés des préoccupations des opérationnels et ainsi de tendre vers une cartographie plus exhaustive. Il s'agit de l'approche ascendante ou encore *approche Bottom-up*. La deuxième approche consiste à recueillir auprès du top management les risques majeurs qui pourraient impacter très fortement l'établissement. Il s'agit de l'approche dite descendante ou encore *approche Top-down.*

Ces deux approches sont complémentaires mais ne nécessitent pas d'être réalisées en même temps. Néanmoins, elles devront faire l'objet d'une étude croisée pour garantir une cohérence et une analyse plus pertinente du niveau de risques qui impacte l'organisation.

Il existe deux types d'approches : top-down et bottom-up

• Approche Bottom-up
Comme évoqué plus haut, favoriser une approche bottom-up va permettre de construire une cartographie plus exhaustive et d'identifier pour chaque processus, tous les événements susceptibles de menacer l'atteinte des objectifs. Il s'agit des risques opérationnels, ainsi que tous les facteurs externes et internes qui en sont les causes mais aussi les facteurs de risques associés. Ainsi, l'utilisation de cette approche encourage l'étude des processus qui composent l'entreprise et de remonter au top management une analyse des activités les plus sensibles.

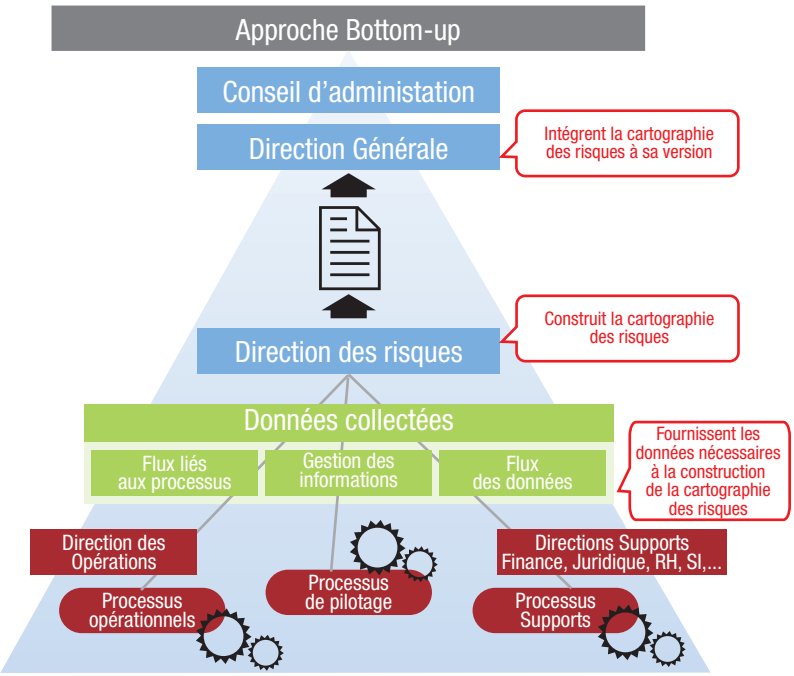
Dans le cadre du dispositif global de gestion des risques et de Contrôle Interne, il est du ressort de la Direction des risques d'apporter le lien nécessaire entre les différentes entités-métiers, supports pour l'identification et l'évaluation des risques et pour la remontée cette information aux organes exécutifs (Direction Générale et Conseil d'administration), de gestion ou de contrôle.

Le pré-requis à l'élaboration de cette démarche est donc l'établissement d'une cartographie et une modélisation
des processus propres de l'entreprise. On distingue trois types de processus :

- Les processus opérationnels : Il s'agit des processus décrivant une ligne de production, la relation avec les bénéficiaires, etc. ;
- Les processus support : Il s'agit des processus décrivant l'établissement des factures ou des fiches de paie par exemple ;
- Les processus de pilotage ou stratégique : Il s'agit des processus conduisant l'établissement à définir ses objectifs et à prendre les décisions stratégiques et tactiques.

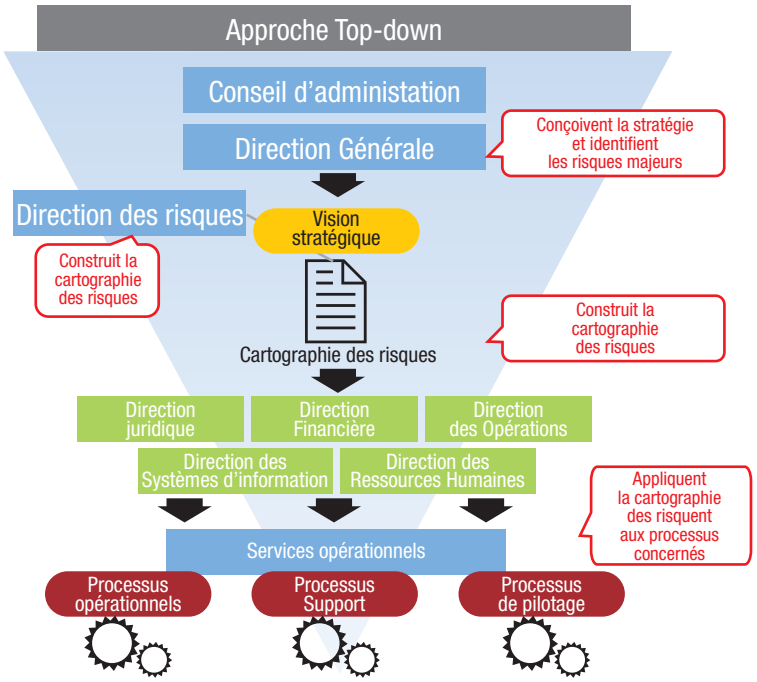
Ce travail permet ainsi de mettre en évidence :

- Les données d'entrées et leurs origines ainsi que les données en sorties et leurs destinations ;
- Les principaux destinataires ou fournisseurs d'informations ;
- Les flux d'entrée et de sortie du processus étudié ;
- Les flux d'échanges et les interfaces entre les processus ;
- Les contrôles nécessaires.



• Approche Top-down
Contrairement à l'approche Bottom-up, cette démarche va privilégier la consultation des membres de l'exécutif afin de recueillir leurs propres appréciations des risques majeurs qui peuvent impactés et détériorer la vision stratégique fixée par le Conseil d'administration et la Direction Générale. L'importance de

cette approche est de proposer aux décideurs une vision globale et stratégique du profil de risque de leur établissement.
Ces risques venant impacter le pilotage de l'entreprise sont par la suite déclinés au niveau des directions métiers dans un premier temps, puis au niveau des services opérationnels c'est-à-dire des processus qui constituent l'activité de l'établissement. Il s'agit de décliner ici les risques stratégiques en risques opérationnels en les rattachant au niveau le plus opérationnel de l'organisation.

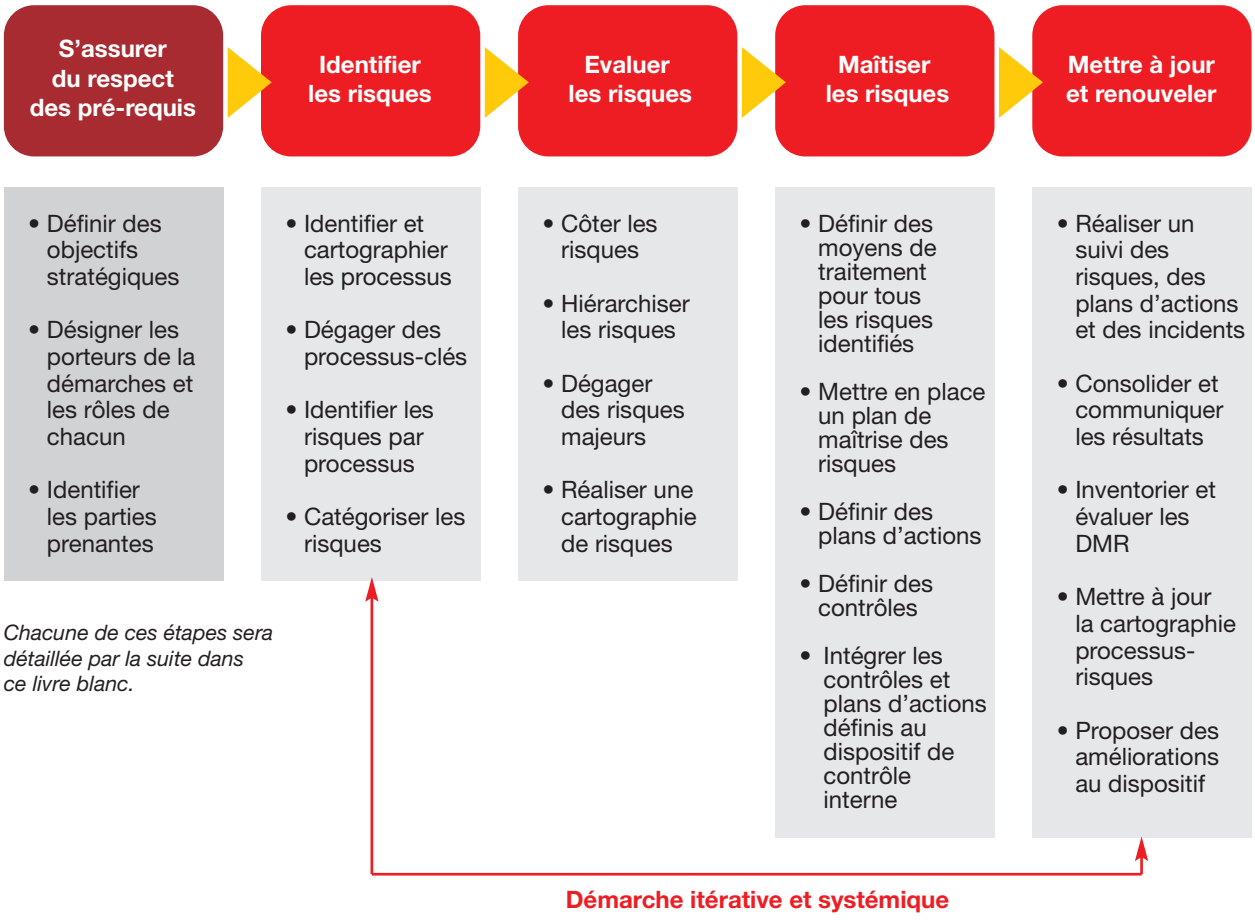


En conclusion, il donc essentiel de faire converger la méthode plus traditionnelle de cartographies des risques des niveaux opérationnels (Bottom-up) avec un mapping plus stratégique (Top-down) à l'initiative des organes de direction, ceci afin de disposer d'un dispositif résolument plus complet et plus efficace.

2. LA MISE EN PLACE DU DISPOSITIF DE CONTRÔLE INTERNE

2.1 Présentation des principales étapes de la méthode

La méthode de maîtrise des risques se découpe en 5 grandes phases comme présenté ci-dessous :



Chacune de ces étapes sera détaillée par la suite dans ce livre blanc.

2.2 Les pré-requis à la mise en place d'un dispositif

Avant de se lancer dans un projet de mise en place d'un dispositif de Contrôle Interne et de maîtrise des risques, il convient de s'assurer que les éléments fondamentaux à la réussite et au bon dimensionnement de la démarche ont bien été identifiés et communiqués et compris par l'ensemble des parties prenantes. Il s'agit pour cela de :

- Décrire et présenter formellement les attentes de la Direction. Cela se traduit par l a définition des objectifs stratégiques et opérationnels que l'exécutif souhaite atteindre, les moyens qu'il met en oeuvre pour y arriver et enfin les bénéfices qu'il souhaite tirer de cette démarche ;
- Désigner le ou les personnes qui assureront le rôle de sponsor de la démarche auprès de la Direction Générale et des directions opérationnelles et supports ;
- Définir les contours des activités opérationnelles et fonctionnelles qui rentrent dans les travaux ;
- Identifier et dimensionner les ressources utiles pour une mise en place rapide et efficace.

2.3 L'identification des risques

2.3.1. L'identification des processus

Une fois les acteurs de la gestion des risques identifiés et les rôles de chacun défini, il s'agit de délimiter le périmètre de la démarche de gestion des risques en définissant les différents processus de l'établissement concerné.

Un processus représente une activité de l'établissement. Les missions d'une structure peuvent être décomposées en autant de processus nécessaires à l'établissement afin de réaliser une représentation fidèle de la réalité du terrain. S'il n'a pas déjà été élaboré, le recensement exhaustif des processus est conduit par l'entité en charge de la démarche dans la structure, voire la Direction Générale ou la Direction de la qualité. Le recensement exhaustif des processus de l'établissement peut comporter plusieurs niveaux de granularité suivant le niveau de détail souhaité. Pour chaque macro-processus, des sous-processus (ou micro-processus) peuvent être identifiés. Ces sous-processus correspondent à un découpage de l'activité en sous-activités, qui représentent souvent les différentes étapes constituant le processus.

Exemple de cartographie de processus :

PROCESSUS	SOUS PROCESSUS
A. Accueil physique du public dans une administration publique	A.1 - Enregistrement et identification du demandeur A.2 - Enregistrement de la demande et orientation A.3 - Réception de l'intéressé par le conseiller technique A.4 - Analyse et intruction de la demande A.5 - Réponse à l'intéressé A.6 - Clôture de la demande

Après avoir restitué une cartographie des processus, il s'agit ensuite d'identifier quels processus sont clés pour l'établissement. Il s'agit en général d'activités critiques pour l'établissement concerné. Ces processus-clés recevront une attention particulière par la suite. La construction d'un référentiel des processus de l'établissement public par la direction en charge de la démarche est nécessaire à la mise en place d'une démarche de maîtrise des risques. Une fois ce référentiel élaboré, il faudra veiller à le maintenir à niveau et à jour en relation avec les différentes directions-métiers. Le recensement des processus peut aussi avoir été fait par le contrôle de gestion ou d'autres directions; il pourra également se faire par un cabinet de conseil externe, qui pourra offrir à la fois son expertise et son indépendance vis-à-vis des structures de l'entité publique.

3.3.2. L'identification et la catégorisation des risques

Cette phase consiste à identifier les risques de l'entité. Une fois la cartographie des processus validée et à jour, il est possible d'associer à chaque niveau le plus fin de processus identifié un ou plusieurs risques. Ces risques sont définis comme « les potentiels événements dommageables qui peuvent remettre en cause le bon déroulement d'un(e) processus/activité ». Dans l'idéal, chaque risque identifié est associé à un processus, qui est lui-même associé à un objectif (de performance par exemple).

Une fois l'identification des risques élaborée, il convient, comme nous le détaillerons par la suite, de consolider les risques principaux en les hiérarchisant. Cette hiérarchisation permet de mettre en lumière les risques majeurs ou critiques pour l'établissement. Ils sont souvent liés aux processus-clés de l'établissement, déjà identifiés lors de l'étape précédente

d'identification des processus. Ces risques sont à traiter en priorité. Ainsi pour le responsable Risques au sein d'un établissement, l'identification des couples « processus critique – risque critique » doit devenir un réflexe.

L'identification des risques par processus peut être facilitée par l'élaboration d'une typologie de risques. Il s'agit de catégoriser chaque risque afin de rendre plus facile sa classification. La séparation classique entre risques financiers et risque extra-financiers peut bien entendu être reprise. Il est ensuite possible de détailler cette typologie en précisant la nature des risques extra-financiers : risque juridique, risque opérationnel, risque image, risque sociétal ou encore risque humain.
Pour le secteur public, nous proposons 6 catégories de risques permettant de classifier la totalité des risques qui peuvent être identifiés :

- Les **risques stratégiques** sont des risques transverses, qui touchent aux processus et activités clés de l'entité publique (par exemple : la défaillance d'un ou plusieurs sous-traitants principaux). Ces risques sont de nature à remettre en cause directement la mission de service public de l'entité concernée. (Somme de risques opérationnels => Risques stratégiques (LB n°1 page 45)
  Les risques stratégiques incluent également les **risques de gouvernance**. Ces risques sont liés aux processus de prise de décision. En l'espèce, ces risques renvoient à la gouvernance même des entités publique, à leurs compétences, celles de leurs agents, ainsi qu'aux interactions entre le politique et l'administratif, et aux règles encadrant les délégations de signature.

N°	Risques stratégiques
1	Echec / Retard / surcoûts d'un projet clés (aménagement infrastructures,…)
2	Echec d'un chantier interne de modernisation ou d'un projet de réforme (transformation, organisation)
3	Dysfonctionnement majeur de la chaîne de décision (articulation entre sphère administrative et politique)
4	Mutation (technologique, institutionnelle, sociétale, …) au sein de l'établissement non ou mal anticipé
5	Défaillance d'un sous-traitant, d'une délégation de service public, etc.

- Les **risques d'image** concernent eux, la notoriété de l'établissement et la façon dont celui-ci est perçu par toutes les personnes extérieures à celui-ci. Un risque d'image apparaît lorsqu'un évènement se produit pouvant impacter de manière négative la réputation de l'établissement public.

N°	Risques d'image
6	Crise médiatique / dénigrement
7	Baisse réelle ou perçue de la notoriété de l'établissement

- Les **risques humains** concernent les risques liés à la gestion des ressources et du public. Ils englobent des domaines aussi divers que la sécurité des hommes (employés, patients, public), l'organisation et la gestion des ressources humaines, les éventuels troubles psychologiques liés au travail, ou la gestion des compétences.

N°	Risques humains
11	Accident majeur dans un établissement (incident, effondrement, …)
12	Accident majeur impliquant un usager du service public (Voirie, accident corporel, …)
13	Comportement inapproprié d'un salarié vis-à-vis d'un usager/patient, (violence, maltraitance, abus de droit, abus de confiance, …)
14	Accident du travail / maladies professionnelles (y compris les risques psychosociaux)
15	Tension sur des catégories de personnel / des compétences critiques (gestion des compétences, recrutement, …)
16	Conflit social (Grève, blocage, …)
17	Absentéisme
18	Perte brutale d'un collaborateur clé

- Les **risques opérationnels** concernent la possibilité de survenance d'un événement dommageable sur un processus opérationnel, ayant pour conséquence la remise en question de la réalisation ou la délivrance du service public. Ils impliquent la mise sous contrôle des processus de bout en bout. En tant que maillons externes de l'établissement public, les personnes privées qui assurent une mission de service public et les structures partenaires doivent aussi être incluses dans la focale d'analyse et de maîtrise du risque opérationnel.

N°	Risques opérationnels
19	Défaillance d'un fournisseur clé (SI, restauration, …)
20	Défaillance critique / indisponibilité des systèmes d'information (paie, serveur de données, …)
21	Perte, vol ou diffusion d'informations sensibles / confidentielles
22	Occupation illicite d'un établissement
23	Interruption durable d'une mission de service public (soin d'un patient, remboursement des frais de soin, …)
24	Fraude interne (salarié) ou fraude externe (usager, patient, …)
25	Erreur / délai dans l'attribution / l'instruction d'une demande d'aide financière

- Les **risques exogènes** englobent tous types de risques dont la principale cause est un facteur extérieur à l'établissement considéré. Les risques de phénomènes naturels ou d'actes malveillants perpétués par une personne extérieure à l'établissement (i.e. terrorisme) sont qualifiés d'exogènes. Dans le cas du secteur public, on peut également inclure dans les risques exogènes, les risques liés à des changements ou des décisions politiques impactant les établissements souvent de façon soudaine et durable.

N°	Risques exogènes
26	Actes de terrorisme
27	Risques naturels / climatiques (tempêtes, inondations, mouvements de terrain, incendie, …)
28	Risques technologiques (risques industriels, transport de matières dangereuses, risques nucléaires, …)
29	Risques sanitaires (pandémie, canicule, ondes électromagnétiques, intoxication, …)
30	Augmentation de l'insécurité (émeutes, agression d'un salarié, …)

- Les **risques juridiques et règlementaires** concernent tous les risques pouvant relever du droit civil, du droit pénal ou du droit administratif.

o Dans le cadre des juridictions civiles et pénales, ces risques concernent le non-respect ou le manquement aux engagements pris dans le cadre de la responsabilité civile (contractuelle ou délictuelle) ou pénale de l'entité publique en tant que personne morale.

o Dans le cadre de la juridiction administrative, ces risques concernent le non-respect des actes administratifs entrant dans le cadre de l'exécution d'une mission de service public (contrats administratifs, décisions individuelles, droit de la fonction publique, etc.)

o Les risques de non-conformité entrent également dans cette catégorie et sont définis comme la possibilité d'un manquement lors de l'application de la réglementation et/ou de la mise aux normes de l'activité d'une entité.

N°	Risques exogènes
31	Non respect de la réglementation / Irrégularité juridique des actes
32	Dysfonctionnement / Erreur dans la passation d'un marché public
33	Evolution défavorable / non anticipée d'une réglementation

2.4 L'évaluation des risques

2.4.1 La méthode de cotation des risques

Une fois identifié, le risque nécessite d'être traité. Pour ce faire, il a besoin d'être correctement évalué. L'évaluation des risques permet ensuite d'identifier les risques majeurs et leur mode de traitement, c'est-à-dire ceux qui remontent à un niveau stratégique. Le directeur général n'a pas besoin d'être informé de l'ensemble des risques existants. La consolidation prend ainsi tout son sens.

Le choix du traitement du risque obéit aux objectifs stratégiques de la collectivité : veut-on le maîtriser en interne ?
Préfère-t-on l'assurer ou le transférer à un tiers ?
Nous nous attarderons ici sur la maîtrise interne des risques, c'est-à-dire sur la mise en place d'un système de Contrôle Interne intégrant à la fois la gestion des risques et les activités de contrôle à proprement parler.

Evaluation du risque brut

Le niveau de risque brut est évalué sur deux axes permettant de définir la criticité du risque :

- L'impact (I) : C'est la conséquence directe et indirecte, immédiate ou in fine, en termes de pertes financières ou de remise en cause des objectifs stratégiques (baisse de revenus, hausse des coûts ou remise en cause des objectifs stratégiques). L'impact peut également prendre en compte les dégradations faites à l'image de l'établissement auprès de ses usagers, patients et autres tiers externes.

IMPACT QUANTITATIF	EQUIVALENCE FINANCIÈRE	EQUIVALENCE IMAGE
1 - Faible	Dépassement < X% du Budget initial	Interruption de service bloquant la bonne exécution d'un processus simple / Atteinte mineure à la crédibilité de l'établissement Détérioration de la relation avec un usager
2 - Modéré	Dépassement entre X% et X% du Budget initial *	Interruption de service bloquant la bonne exécution d'un processus transverse / Atteinte marquée à la crédibilité de l'établissement Détérioration de la relation avec un usager important
3 - Important	Dépassement entre X % et X% du Budget initial	Manquement aux missions secondaires de l'établissement / Recours devant les juridictions civiles et administratives à l'encontre de l'établissement. Couverture médiatique locale
4 - Critique	> X% du Budget initial*	Manquement grave aux missions fondamentales de l'établissement / Poursuite judiciaire pénale à l'encontre d'un membre de la direction. Couverture médiatique nationale

** Budget initial : Budget pour lequel l'équilibre budgétaire de l'entité publique est conservé*

- La probabilité (P) : Il s'agit de l'appréciation de la probabilité de survenance du risque dans le temps. Cette probabilité peut être définie selon un volume d'activité ou en termes de fréquence suivant les risques évalués.

PROBABILITÉ	EQUIVALENCE TEMPORELLE	EQUIVALENCE VOLUME
1 - Faible	Annuel	< X% du volume de référence*
2 - Modéré	Semestriel	Entre X% et X% de volume de référence*
3 - Important	Mensuel	Entre X% et X% de volume de référence*
4 - Critique	Hebdomadaire	> X% du volume de référence*

** Exemples : temps de travail, nombre de dossier traités, etc.*

Dans cet exemple nous avons présenté une évaluation des impacts selon deux axes. Il est possible d'ajouter d'autres axes d'analyse en fonction de vos besoins (Ex. : Equivalence légale/juridique, > équivalence informationnelle, etc.). Néanmoins, il est nécessaire de limiter le nombre d'axes d'analyse pour ne pas complexifier la méthodologie de maîtrise des risques.

Le niveau de risque est le produit matriciel de la moyenne des impacts par la probabilité de survenance :

$$\text{Risque brut} = \left\{ \frac{\sum \text{impacts}}{\text{n impacts}} \right\} \text{ x probabilité}$$

Cotation nette

Au travers de l'évaluation du risque net, il s'agit de mesurer l'exposition réelle de l'établissement compte tenu soit des moyens de maîtrise des plans d'actions ou des moyens de prévention et/ou de détection mis en oeuvre.

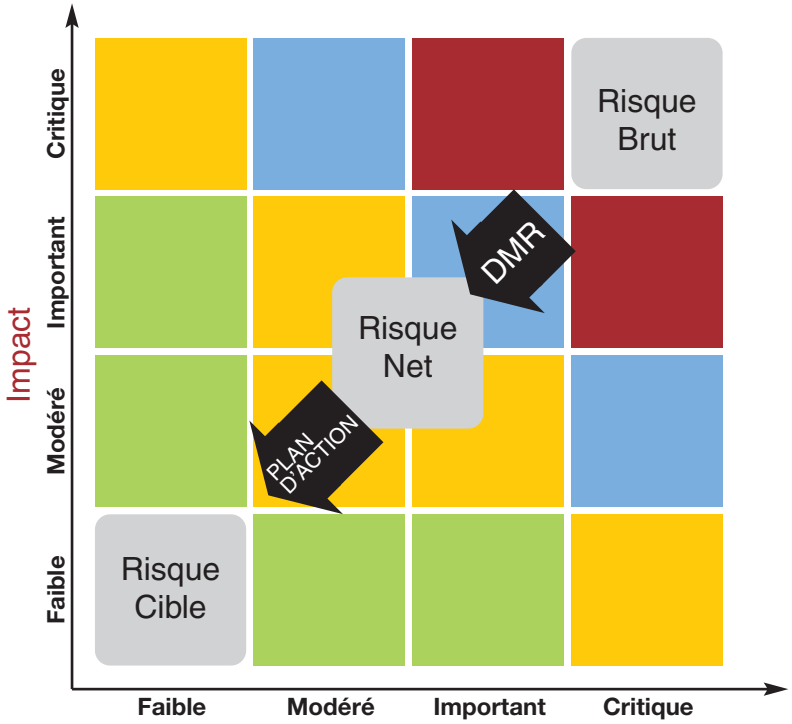
La formule d'évaluation du risque net pourrait se présenter de la manière suivante :

$$\text{Risque net} = \left\{ \frac{\text{Risque Brut}}{\text{Niveau de maîtrise}} \right\}$$

Le niveau de maîtrise correspond à l'évaluation de l'efficacité et de la pertinence du Dispositif de Maîtrise des Risques. Nous reviendrons plus en détail sur cette évaluation dans le paragraphe 1.2.3.5.3.

Matrice de criticité du risque

- **Risque prioritaire**
- **Risque élevé**
- **Risque à surveiller**
- **Risque faible**



RISQUE INHERENT ET RISQUE RESIDUEL LES VISEES PEDAGOGIQUES DU CALCUL DE LA CRITICITE DU RISQUE

La criticité d'un risque *(probabilité d'occurrence x impact) s'évalue à deux reprises au cours d'un exercice de la démarche : au début, lors de la réalisation de la cartographie ; à la fin, pour actualisation. La première évaluation correspond au risque inhérent, ou risque brut ; la seconde évaluation correspond au risque résiduel ou risque net.*

La valeur du risque brut *correspond à la criticité du risque pour lequel aucun élément de maitrise n'a été mis en place pour en diminuer les effets.*

La valeur du risque résiduel ou risque net *correspond à la valeur du risque après la mise en place d'un dispositif de maîtrise des risques (DMR) de type protection et/ou de prévention.* ***La protection*** *va permettre de diminuer la gravité, en limitant ce que pourrait être l'impact du risque en cas d'accident.* ***La prévention*** *va permettre de diminuer la probabilité de survenance du risque.*

Sur la cartographie des risques, les DMR de protection vont avoir pour effet une ***translation horizontale*** *du risque et les DMR de prévention vont avoir pour effet une* ***translation verticale*** *du risque.*

Après évaluation du ***risque résiduel,*** *les responsables de la démarche échangent avec le "propriétaire" du risque, c'est-à-dire le responsable de son évaluation et des actions de maîtrises sur ce risque, pour vérifier avec lui l'applicabilité et l'efficacité des contrôles.*

Dans le cas où les contrôles ne sont pas appliqués ou s'ils ne sont pas pertinents au regard de la nature du risque, le responsable de la démarche réévalue la criticité du risque résiduel.

Si le risque résiduel correspond au risque cible : le risque doit être surveillé et faire l'objet d'une revue.

Si le risque résiduel ne correspond pas au risque cible : le risque doit faire l'objet d'un traitement additionnel avec la mise en place de plans d'actions complémentaires.

Cette démarche est ensuite formalisée et permet le calcul systématique et organisé de la criticité des risques (risques inhérents et risques résiduels) et, de justifier les actions de contrôle. Elle permet d'autre part de montrer aux directeurs opérationnels et "propriétaires" de risques le fonctionnement, dans son aspect pratique, de la gestion des risques. La vocation pédagogique de la démarche participe à l'appropriation de la gestion des risques et du Contrôle Interne par les agents opérationnels et les directions métiers.

A noter toutefois que dans la pratique, l'analyse se fait parfois uniquement sur les risques nets en intégrant ainsi directement dans l'analyse les mesures déjà prises.

2.4.2 L'élaboration de la cartographie des risques

La cartographie des risques est un outil permettant de recenser l'ensemble des risques pouvant perturber l'atteinte
des objectifs de l'établissement et de les prioriser en fonction de leur criticit.. Elle est la base du processus de ngestion des risques car elle alimente le référentiel de contrôles et permet donc la sécurisation des processus.

Afin de transformer cet inventaire en véritable outil d'aide à la décision, un effort de priorisation et de hiérarchisation des risques doit être mené. En effet, après une première étape d'identification et d'évaluation des risques, l'enjeu de la démarche réside dans la priorisation des risques afin de faciliter la prise de décision quant aux priorités de traitement.. Ce travail permet ainsi de présenter une vision synthétique et pertinente au plus près des préoccupations opérationnelles et stratégiques de l'établissement.

En donnant à la démarche tout son aspect stratégique, la consolidation est donc une étape clé car elle propose une vision d'ensemble, dépouillée des éléments non suffisamment structurants.

L'étape de consolidation revient à regrouper, dans une même représentation visuelle – la cartographie (Heat Map) - l'ensemble des risques susceptibles de venir affecter les directions métiers et les directions supports mais aussi la Direction Générale de l'établissement. Au travers de la cartographie, une première hiérarchisation des risques est réalisée en sélectionnant les plus significatifs, tout en écartant ceux jugés peu pertinents au niveau global car perçus comme très opérationnels et sans impact suffisamment significatif. La consolidation doit aboutir à une nouvelle cartographie, « synthèse intelligente » des cartographies des directions.

Il s'agit ici, d'identifier les risques qui devront faire l'objet d'une remontée à la Direction Générale (Approche Bottom-up). Il est ici l'heure des choix : établir une hiérarchie des risques ; remonter les risques majeurs[9] à la direction ; prioriser les actions à mener sur ces risques.
La consolidation répond à plusieurs desseins majeurs :

- Elle permet à la Direction Générale de disposer d'une vision stratégique des risques de l'établissement ;
- Elle permet aux pilotes du dispositif de gestion des risques et de Contrôle Interne d'identifier les priorités concernant le traitement des risques (pour ainsi se concentrer sur les risques majeurs) ;
- Autre enjeu de la consolidation : lors de la réalisation des entretien (Top Down ou Bottom Up), la vision par interlocuteur peut aboutir à un nombre de risques importants avec des niveaux de granularité disparates, des redondances et parfois des cotations différentes pour un même risque, d'où la nécessité d'homogénéiser les niveaux d'analyse et les cotations et d'arbitrer sur les risques qui composeront la cartographie.

La consolidation implique une sélection des risques qui sont perçus comme majeurs si l'on se place selon le spectre d'une Direction Générale.

La sélection s'opère sur la base des cartographies des directions métiers et supports par la fonction en charge d'animer le dispositif de Contrôle Interne. Cette sélection tient compte bien sur du profil de risque de l'établissement et de l'appétence de l'équipe dirigeante et des membres du Conseil d'administration de l'établissement. Cette sélection doit faire preuve de pertinence et justifier auprès de l'exécutif du choix des critères de consolidation :
risques récurrents, risques à impact potentiel élevé, risques diffus mal identifiés, etc.
La cartographie des risques consolidée est le principal support de gestion des risques remis à la Direction Générale, en restant attentif à deux écueils :

- Certains risques particuliers ou spécifiques à un périmètre donné sont difficiles à consolider, a contrario des risques transverses à toutes les activités de l'établissement ;
- La consolidation a une visée stratégique et générale mais n'a pas de portée opérationnelle. Bien souvent,

les directions métiers et supports n'ont pas besoin de cartographie consolidée ; pour elles, l'essentiel se joue au niveau opérationnel. Néanmoins, elle reste un outil stratégique destiné à la Direction Générale.

2.5 Les Dispositifs de Maîtrise des Risques (DMR)

2.5.1 Inventaire des Dispositifs de Maîtrise des Risques

L'identification des moyens de maîtrise doit permettre une meilleure appréciation du niveau de risque auquel est exposé l'établissement. Cependant, il n'existe pas de corrélation formelle entre un niveau de maîtrise et un niveau de risque net, chacun étant évalué à dire d'expert selon les principes d'objectivité et de transparence qui régissent la démarche de maîtrise des risques.

Les éléments de maîtrise qui composent le dispositif de maîtrise global peuvent se présenter selon 3 natures permettant ainsi de préciser la stratégie de maîtrise utilisée par l'établissement pour maîtriser son risque.
Les trois natures les plus communément utilisées sont :

- Préventif : l'élément de maîtrise permet de prévenir le risque avant sa réalisation ;
- Détectif : l'élément de maîtrise permet d'identifier rapidement la réalisation concrète du risque ;
- Curatif : l'élément de maîtrise permet d'amoindrir ou de transférer les conséquences de réalisation du risque.

Par la suite, pour chaque élément de maîtrise, il convient de définir une fréquence de réalisation. Il s'agit ici, de déterminer à quelle périodicité le moyen de maîtrise va être réalisé dans un cadre opérationnel normal. Cette fréquence sert ensuite de référence pour la planification et l'échantillonnage des tests ponctuels réalisés par les équipes Risque ou de l'Audit Interne. Les fréquences les plus couramment utilisées sont les suivantes : sur flux, quotidien, hebdomadaire, mensuel, trimestriel, semestriel, annuel, sur demande.

Evaluation des DMR
Chaque organisme est libre de proposer et concevoir sa propre méthode d'évaluation de son dispositif de maîtrise des risques. Dans le cadre de ce livre blanc, sont proposés 4 critères qui peuvent rentrer dans cette évaluation :

- **La réalisation :** l'élément de maîtrise est effectivement réalisé conformément à ce qui est prévu dans le cadre d'une activité normale. Trois situations standards sont définies :
  - o **Réalisé entièrement** : l'élément de maîtrise est toujours réalisé à la bonne période et conformément à son mode opératoire prévisionnel ;
  - o **Réalisé partiellement** : l'élément de maîtrise est réalisé, mais sa réalisation ne respecte pas la périodicité ou le mode opératoire prévisionnels ;
  - o **Non réalisé** : dans les faits, l'élément de maîtrise identifié n'est pas réalisé, ou très rarement.
- **La traçabilité** : lors de sa réalisation, l'élément de maîtrise produit une preuve d'audit permettant de le tracer si besoin. Trois possibilités standards sont définies :
  - o La traçabilité papier : l'élément de maîtrise génère un document papier identifiable et stocké attestant de sa réalisation et du résultat obtenu ;
  - o La traçabilité informatique : l'élément de maîtrise génère un document numérique identifiable et stocké attestant de sa réalisation et du résultat obtenu ;
  - o Non traçable : aucune preuve ne subsiste une fois l'élément de maîtrise réalisé.
- La formalisation : l'élément de maîtrise est formalisé par un document ou une procédure écrite, validée et partagée.
- La faisabilité : l'élément de maîtrise est correctement dimensionné au regard la gravité et de la survenance du risque (Cf. : moyen humain mis à disposition, enveloppe budgétaire, etc.).

A l'issu de l'évaluation des 4 critères vus ci-dessus, il faut alors se poser la question de la conception du DMR, à savoir, est-il :

- o **Pertinent :** la conception de l'élément de maîtrise répond parfaitement aux exigences de maîtrise du risque associé ;
- o **Améliorable :** la conception de l'élément de maîtrise correspond partiellement aux exigences de maîtrise du risque associé et peut être amélioré ;
- o **Inutile :** la conception de l'élément de maîtrise ne répond pas aux exigences de maîtrise du risque associé rendant ainsi l'élément de maîtrise inutile dans le cadre de la démarche.

2.5.2 Les contrôles
Une fois la cartographie des risques consolidée et validée, le responsable du dispositif de Contrôle Interne, en relation étroite avec la

Direction Générale et le Conseil d'administration, choisit pour chaque risque majeur identifié, la politique de traitement qu'elle souhaite mettre en place. La Direction Générale apportera une attention toute particulière aux risques majeurs pour lesquels elle a auparavant défini un seuil. Toutefois, son attention doit également se porter sur les risques moins impactant pour l'établissement mais dont la maîtrise relève d'avantage de la responsabilité des directions métiers et supports. Avec l'accompagnement du responsable du dispositif de Contrôle Interne, ils leur appartiennent de définir et de mettre en oeuvre les actions de prévention et de protection nécessaires pour sécuriser les processus de leur ligne métier. Ces actions font par la suite l'objet d'une vérification permanente par le Contrôle Interne (Contrôle de deuxième niveau) et périodiquement par l'audit interne (Contrôle de troisième niveau).
Au cours de ses missions d'audit sur une thématique précise, l'audit interne peut ainsi rendre compte du niveau de maîtrise et le cas échéant proposer des recommandations pour améliorer l'efficacité et la pertinence des contrôles mis en place.

Les types de contrôles
Le système de Contrôle Interne tel que présenté dans ce livre blanc prévoit, au sein de l'activité de traitement des risques, la mise sous contrôle du risque en tant que tel. Le COSO définit la mise sous contrôle comme « une mesure de prévention, de protection et de détection du risque ».
Les contrôles peuvent être de différentes natures et prendre plusieurs formes. Ils peuvent être mis en place à des niveaux hiérarchiques différents. Ainsi, les opérations de contrôle peuvent être présentées de manière synthétique sur trois niveaux comme suit :

- Le premier niveau de contrôle est effectué par l'opérationnel, au moment de l'exécution de sa tâche.
  L'agent connait et décline les actions qu'il a à mener et les procédures qu'il a à suivre (en termes de sécurité par exemple) dans la réalisation quotidienne de son travail.

- Le second niveau est un contrôle a posteriori, qui peut prendre plusieurs formes (potentiellement cumulatives) :
  - contrôle ponctuel effectué par l'opérationnel (après échantillonnage par exemple, lors de campagnes d'auto-évaluation)
  - hiérarchique effectué par le management intermédiaire ;
  - contrôle spécifique effectué par un responsable fonctionnel : contrôle interne, contrôle de gestion, management de la qualité, direction de la sûreté, etc. ;
  - contrôle effectué par un tiers (interne ou externe à la structure).

- Le troisième niveau est un contrôle périodique, qui relève généralement de la responsabilité de l'audit interne, dont le but est de "s'assurer que le contrôle a été effectué", qu'il est cohérent et efficace par rapport au risque concerné. Il peut déceler les éventuelles failles dans les autres niveaux du contrôle. Ce troisième niveau évalue la solidité des deux premiers.

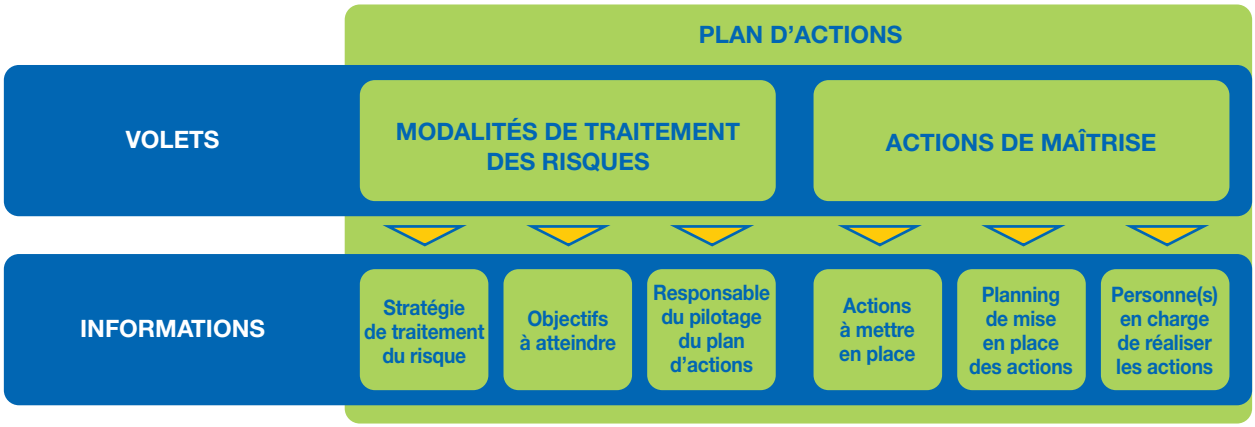
Pour accompagner la mise en place d'un dispositif de Contrôle Interne efficace et efficient au sein de l'organisation, des filières (c'est-à-dire un réseau de coordinateurs de Contrôle Interne présent au sein de chaque direction métier et opérationnelle) de contrôle par activité ou par risque peuvent être créées. Véritable relais opérationnels pour la Direction du Contrôle Interne, ces filières ont pour fonction de recueillir les informations qu'elles jugent pertinentes et nécessaires pour le contrôle des différents processus.

A la tête de chaque filière, un correspondant est nommé. Véritable chef d'orchestre opérationnel, le correspondant du Contrôle Interne a la charge d'animer la filière et de s'assurer du bon déroulement de la méthodologie de Contrôle Interne et d'orienter les décisions. Il est également le garant du respect des procédures de contrôle au sein de sa filière.
Les filières qui composent le dispositif de Contrôle Interne favorisent, de part leur interaction entre elles, une circulation de l'information à la fois transverse et horizontale au sein de l'organisation.

2.5.3 La gestion des plans d'actions
Une fois la cartographie des risques réalisée et les dispositifs de maîtrise des risques identifiés, il s'agit de traiter les risques non couverts et de proposer des solutions de traitement pour chacun des risques identifiés.

(9) L'utilisation du terme "stratégique" (voire risques "macro") est préférable à celui de "majeur" qui est aussi utilisé pour la cotation (criticité) du risque dans le sens, par exemple, de mineur, modéré, significatif et majeur

La définition des plans d'actions

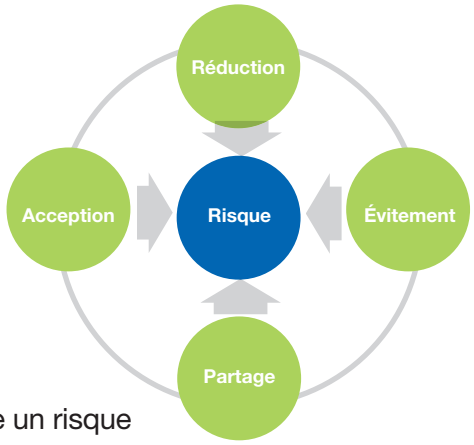


Un plan d'actions s'organise en deux volets :

- En premier lieu, il s'agit de définir pour le(s) risque(s) concerné(s) les modalités de traitement ;
- En second lieu, il s'agit de définir des **actions de maîtrise** à mettre en place afin de maîtriser le(s) risque(s) concerné(s)

Pour chacun de ces volets, un certains nombre d'informations doit être collecté : les responsables, les objectifs à atteindre, la stratégie choisie, les actions à prendre, etc.

La première étape de définition d'un plan d'actions consiste à choisir les modalités de traitement d'un risque, notamment la stratégie à adopter. En pratique, on distingue quatre grandes stratégies de traitement des risques, détaillés dans le schéma ci-dessous :



- Réduire un risque

La réduction d'un risque peut se faire de plusieurs façons : on peut choisir de **réduire sa probabilité d'occurrence** ou **de réduire son impact.**

o La mise en place d'un contrôle en tant qu'action de maîtrise va par exemple permettre de réduire sa probabilité d'occurrence.

o La mise en place de procédures en cas de survenance d'un risque peut également permettre de réduire l'impact de celui-ci. Dans le cas du risque d'incendie au sein d'une structure accueillant des employés ou du public, le risque va ainsi être réduit si des mesures anti-incendie sont mises en place : procédures d'évacuation en place, installations conformes aux normes de sécurité (extincteurs, sprinklers, portes coupe-feu…), responsables incendie désignés parmi le personnel, etc. Une fois ces procédures mises en place, on parle de dispositifs de maîtrise de risques (DMR) qu'il faut maintenir sur le long terme.

- Eviter un risque

Une stratégie d'évitement peut également être choisie afin de traiter un risque. On peut choisir de supprimer la cause du risque si celle-ci est clairement identifier ou encore de transférer ce risque vers un acteur extérieur à l'établissement :

o Si la cause d'un risque est clairement identifiée, elle peut donc être supprimée. Par exemple, un risque de fraude existe car trop d'activités sensibles sont concentrées entre les mains d'un seul employé ou d'un groupe d'employés. Mettre en place une politique de séparation de fonctions permet ainsi de réorganiser le département/service afin de ventiler les activités sensibles entre différentes personnes ou différentes groupes de personnes. Cette action permet ainsi de réduire drastiquement le risque ou de le supprimer totalement.

o On peut également éviter un risque en le transférant vers un acteur extérieur à l'éta-

(9) L'utilisation du terme "stratégique" (voire risques "macro") est préférable à celui de "majeur" qui est aussi utilisé pour la cotation (criticité) du risque dans le sens, par exemple, de mineur, modéré, significatif et majeur

blissement. Il peut s'agir d'un fournisseur, d'un sous-traitant, d'un délégataire, d'un organisme d'assurance, etc.

Lorsque le risque est transféré vers un organisme d'assurance, on parle d'une stratégie de financement du risque : en cas d'occurrence, les pertes financières seront couvertes par l'organisme de l'assurance plutôt que par l'établissement.

- Partager un risque
  Le transfert d'un risque ne peut être que partiel, on parle dans ce cas d'un partage de risque. Dans le cas d'un processus partiellement pris en charge par un fournisseur par exemple, le risque de défaillance lié à ce processus sera partagé par l'établissement et le fournisseur.

- Accepter un risque
  Il arrive qu'un risque soit accepté, on choisit alors de ne pas traiter un risque : aucun contrôle, aucune modification d'organisation, d'activité ou de procédure n'est prévue afin de prévenir le risque.
  Le risque accepté se trouve ainsi dans les limites d'appétence aux risques de l'établissement. Celui-ci n'est pas considéré assez critique, ou sa probabilité d'occurrence assez élevée pour que celui-ci soit traité.
  Dans le cas des entités publiques, on peut citer le risque de changement de politique du gouvernement qui peut ainsi impacter durablement les stratégies des entités, mais qui est accepté tel quel par nombre d'entre elles.

LA NOTION D'APPETENCE AUX RISQUES DANS QUELS CAS UN RISQUE EST-IL JUGÉ ACCEPTABLE ?

L'appétence aux risques est une notion qui apparaît dans les référentiels de Contrôle Interne du COSO. Celle-ci est définie comme « le niveau de risques qu'une organisation est prête à accepter ».

Le niveau de risques ou degré d'appétence au risque qu'une organisation est prête à accepter repose davantage sur la catégorie de risque que sur sa gravité : les organisations semblent en effet prêtent à prendre des risques lorsque ceux-ci sont externes (Ex. : environnement concurrentiel, marchés financiers, financement d'une innovation de rupture) contrairement à ceux qui seraient internes (Ex. : Santé & sécurité, conformité, etc.).

Une appétence élevée aux risques pour une organisation ne signifie pas que celle-ci ne doive pas mettre en place de démarche de gestion les risques intégrant un reporting régulier et une stratégie de surveillance et/ou de mise sous contrôle de ses risques et de leurs conséquences.

Lorsque qu'une entité cherche à déterminer son niveau d'appétence aux risques, il lui faut prendre en compte différents facteurs :

***Sa stratégie globale** – quelle est la stratégie adoptée ? Celle-ci intègre-t-elle des activités nouvelles pour l'entité comprenant une grande part de risques (i.e. innovation, etc.) ?*

Son profil actuel de risque *– quel est le niveau de risque de l'entité et comment les risques sont-ils distribués et gérés au sein de l'organisation ?*

***Sa capacité à faire face aux risques** – Quelle est la part de risque que l'organisation est capable de supporter dans la poursuite de ses objectifs stratégiques ?*

***Sa tolérance aux risques** – Quel est le niveau de risque que l'entité est disposée à accepter afin de remplir ses objectifs ?*

***Son attitude face aux risques** – quelle est l'attitude de l'entité face aux risques, à sa croissance et au retour sur investissement qu'elle attend ?*
En fonction de ces facteurs, l'organisation va être en mesure de se placer sur une échelle d'appétence aux risques dont les niveaux peuvent être définis comme suit : aversion aux risques, acceptation minimale, acceptation prudente, ouverture aux risques, avidité face aux risques.

Le niveau d'appétence aux risques des entités publiques tendra généralement vers un niveau d'appétence aux risques très limité, particulièrement dans les domaines suivants : sécurité des biens et des personnes, conformité

Ainsi, pour chaque risque identifié auquel on prévoit de lier un plan d'action, il faudra sélectionner une stratégie de traitement. Il faudra ensuite définir un objectif à atteindre à la fin du plan d'action.
Une fois la stratégie de traitement du risque sélectionnée, il s'agit de définir les actions de maîtrise en fonction du risque mais aussi de la capacité des services concernés à les mettre en oeuvre. Les actions de maîtrise choisies doivent être réalisables pour tous les acteurs concernés et cohérentes avec la stratégie globale de l'entité publique ainsi que les objectifs stratégiques de chacun.
Plusieurs types d'actions peuvent être définies (cette liste n'est pas exhaustive) :

- Mettre en place des contrôles qui seront par la suite intégrés au dispositif de Contrôle Interne ;
- Mettre en place des procédures de prévention, ou des procédures de gestion des incidents ;
- Mener des réorganisations en interne ;
- Mener des actions de formation ou de sensibilisation ;
- Mettre en place des canaux d'alertes ;
- Mettre en place des services de supports (psychologique dans le cas des risques psychosociaux, etc.).

Plusieurs actions ou types d'actions peuvent être combinées afin d'atteindre l'objectif fixé par le plan d'actions.

La mise en place des plans d'actions
Une fois la stratégie de traitement du risque et les actions à mettre en oeuvre définies, il s'agit de déployer ces actions sur le(s) périmètre(s) concerné(s). Un plan d'actions peut effectivement être décliné de différentes manières au sein de l'entité suivant ses besoins : verticalement, au sein d'une ou plusieurs directions ou horizontalement au sein d'un processus.
Ainsi, un plan d'actions décliné par processus concernera la totalité des activités réalisées dans le cadre de ce processus. De ce fait, il est possible que la mise en place de ce plan d'actions se fasse de manière transverse, car concernant les activités de plusieurs départements rattachés à plusieurs directions opérationnelles ou directions support différentes.
Un plan d'actions peut également être mis en place verticalement, au sein d'une direction ou plusieurs directions, sur une partie ou la totalité des activités entrant dans le périmètre des ces directions.
La mise en place d'un plan d'actions est facilitée par la désignation d'un responsable, en charge de piloter le déploiement des actions de maîtrise des risques. Celui-ci aura en charge le respect du planning ou de l'échéance définie, et la coordination des différentes actions prises dans le cadre du plan d'actions. Des correspondants locaux peuvent aussi être désignés et ainsi prendre en charge une ou plusieurs actions sur leur périmètre local, afin de faciliter la mise en place des actions de maîtrise dans le cas où le plan d'actions s'appliquerait de manière transverse à plusieurs services/directions/ départements.
Pour chaque plan d'actions, il est également utile de définir un planning de réalisation avec une échéance à respecter. Le respect ou non de cette échéance permettra de mesurer si le plan d'actions est cohérent, réalisable, et efficace, et en fonction de ces résultats, d'adapter la démarche de maîtrise des risques.

Le suivi des plans d'actions
Un suivi des plans d'actions est nécessaire afin de mesurer les résultats obtenus, et d'améliorer le dispositif. Une fois le plan d'action mis en place, il est utile de réévaluer le risque concerné par le plan d'action afin de mesurer sa nouvelle criticité, et ainsi vérifier si la cible a bien été atteinte.
Le suivi des plans d'actions devra être réalisé par la cellule de Contrôle Interne. Des modalités de remontée d'informations devront être définies en amont afin d'assurer le suivi du plan d'actions. Généralement, les remontées d'informations peuvent être effectuées ou pilotées par le responsable du plan, qui s'assurera ainsi que des rapports d'avancement et un reporting sur les actions entreprises sont régulièrement transmis au Contrôle Interne.
Une fois l'échéance atteinte, un bilan global du plan d'actions devra être réalisé. Il devra rendre compte des résultats obtenus, des difficultés rencontrées et de la pertinence globale du plan d'actions vis-à-vis du/des risque(s) couvert(s) et des processus concernés. En fonction de ce bilan, le plan d'actions pourra être réévalué, révisé ou mis à jour. L'analyse faite a posteriori de la mise en place du plan d'actions permettra aussi d'apporter des améliorations à la méthode d'implémentation des plans d'actions participant ainsi à l'amélioration de la méthodologie globale de gestion des risques et de Contrôle Interne.

2.6 La mise à jour et le renouvellement du dispositif : la transformation de la démarche en instrument de performance

La réduction des risques est une des composantes de l'amélioration de la performance, qui elle vise à réduire les délais, les coûts et les dysfonctionnements. Cependant, toute démarche d'amélioration des processus repose sur une connaissance de l'activité. C'est la raison pour laquelle, cette démarche doit être accompagnée par la mise en place d'une base incidents dont l'objectif est de fournir des informations précieuses sur les risques avérés. La mise en place d'une base d'incidents (ou base de pertes) constitue un très bon instrument de mesure de la performance puisqu'elle va permettre de donner une vision passée des risques avérées et permettre ainsi d'anticiper, prévenir les risques futurs et d'avoir une meilleure connaissance des zones de vulnérabilité pouvant déstabiliser votre organisation.

2.6.1 La gestion des incidents

Les incidents sont des événements qui engendrent ou traduisent des dysfonctionnements dans le déroulement factuel d'un processus. En d'autres termes, l'incident est de fait la matérialisation d'un risque donné, que l'on appelle également « risque avéré ».
Dans le cadre du renforcement du dispositif de Contrôle Interne de l'établissement, la mise en place d'une base d'incidents permet de compléter le processus de maîtrise des risques et d'évaluer l'exigence de fonds propres relative aux risques opérationnels.

La collecte des incidents

Les objectifs de la collecte des incidents dans une base dédiée sont multiples. Il s'agit de :

- Saisir des incidents liés à l'occurrence d'événements de risques opérationnels avec pour chacun d'entre eux l'identification de l'entité et du processus concerné, de la cause et des conséquences de l'incident, ainsi que l'estimation des pertes associées ;
- Analyser a posteriori les incidents déclarés consécutivement à la survenance d'un risque opérationnel ;
- Consolider les données à des fins de reporting interne et externe ;
- Identifier, décrire et suivre les éventuels plans d'actions jugés nécessaires pour améliorer la maîtrise des risques en les reliant aux incidents auxquels ils sont censés apporter des réponses ;
- Rapprocher ces incidents avec la cartographie des risques, afin de disposer de toutes les données quantitatives et qualitatives nécessaires à :
  - o La meilleure gestion du risque opérationnel et la mise en place de mesures correctives adaptées ;
  - o La quantification et la modélisation du risque opérationnel.

La déclaration d'incidents

Un incident opérationnel est un événement qui provoque des dysfonctionnements dans le déroulement normal d'une activité ou d'un processus se traduisant par un impact financier ou non. L'incident est la matérialisation d'un risque donné. C'est par exemple une panne informatique, une erreur de saisie de données, une fraude interne ou encore une catastrophe naturelle.
Il est possible de classifier les incidents suivant les typologies de risques suivantes :

- **Fraude interne :** Vol ou délits d'initié ;
- **Fraude externe :** Actes de fraude de la part d'un tiers (Ex. : dommages dus au piratage informatique) ;
- **Pratiques en matière d'emploi et de sécurité sur le lieu de travail :** Relation de travail, égalité, discrimination ;
- **Pratiques relatives aux bénéficiaires, produits, activités commerciales :** défaut de conseil, violations relatives à des données personnelles, détournement d'argent ;
- **Dommages aux actifs corporels :** Catastrophes et autre sinistres ;
- **Dysfonctionnements de l'activité et des systèmes :** Pannes de matériel ou de logiciels informatiques, défaillances des systèmes de télécommunication ;
- **Exécution des opérations, livraisons et gestion des processus :** Erreur d'enregistrement des données, défaillances des fournisseurs.

Généralement, le principe de collecte des incidents est déclaratif et décentralisé au sein de chaque entité opérationnelle. L'entité déclarante est donc responsable du contenu des informations qui sont communiquées dans le cas de la remontée d'un incident. Aussi, il est impératif que le processus de remontée d'incident respecte certains principes :

- **Fiabilité :** Les informations saisies dans la fiche incident ou dans l'outil dédié doivent être conformes à la réalité ;

- **Exhaustivité :** L'ensemble des pertes liées à la réalisation de l'incident doit être remonté ;

- **Auditabilité :** Dans le cadre d'un audit interne ou externe ou à la demande de la Direction du Contrôle Interne, les données sources ayant permis de saisir l'incident et la piste d'audit des modifications, mises à jour devront être connues et accessibles.

La collecte des incidents étant ouverte à l'ensemble des collaborateurs de l'établissement, il est recommandé de fixer des règles et notamment des seuils pour éviter de recueillir des incidents dont l'impact est faible ou quasi nul et viendrait « polluer » la base incidents.

La mise en place d'un seuil plancher de collecte permet généralement que la base de données contienne uniquement des incidents significatifs. Il importe à chaque établissement de fixer son seuil en fonction de son volume d'activité.

Même si la règle doit demeurer la saisie unitaire et au fil de l'eau de chaque incident pris comme un événement indépendant, il est recommandé de procéder à une agrégation pour les incidents de faible montant mais ayant une fréquence élevée.

La quantification d'incidents

Un incident est un risque avéré dont il possible de décrire les causes réelles et les conséquences directes et
indirectes permettant ainsi de déterminer un impact financier.

Par convention, un incident peut être qualifié selon trois typologies ;

- Une perte : Il s'agit d'un impact négatif sur les bénéfices ou les actifs de l'établissement. Par exemple :
  - o Impacts directs : Pertes liées à un vol, pénalités relatives à un retard de traitement ;
  - o Impacts indirects liés à l'investigation : Coût en jours/homme relatif à la résolution de l'incident.
- Un gain : Il s'agit d'un impact positif sur les bénéfices ou les actifs de l'établissement. Par exemple :
  - o Passage d'un ordre en bourse, différences de change, etc.
- Sans impact financier

L'appréciation d'un incident peut être réalisée selon deux axes d'analyse :

- **Les causes :** Une bonne compréhension des causes d'un incident permet de prévenir l'établissement d'une nouvelle survenance ou bien d'en limiter ses conséquences. Il incombe à chaque établissement de définir sa propre typologie de causes en fonction de son activité et de son retour d'expérience en la matière. Il est important de noter qu'une seule cause peut entraîner plusieurs conséquences, qui ellesmêmes peuvent avoir à leur tour plusieurs effets. Il est également possible qu'un événement ait pour origine des causes multiples conjuguées.

- **Les conséquences :** Un incident peut engendrer une ou plusieurs conséquences financières mais également des conséquences non financières que nous pourrions qualifier de qualitatives. Ces dernières peuvent être grave et porter atteinte à la réalisation de la mission de service public. Il s'agit par exemples des conséquences judiciaires (assignation par un tiers), matérielles (incidence sur la santé et la sécurité) ou bien d'image/réputation (insatisfaction des bénéficiaires).

Le suivi des incidents

La collecte des incidents est un processus décentralisé au plus près de leur survenance, c'est-à-dire au niveau des
entités opérationnelles et supports de l'organisation. Chaque collaborateur de l'établissement peut détecter un incident et le déclarer. Ainsi, la déclaration qui se fait au fil de l'eau, peut être faite par la « Victime », « l'Auteur » ou encore par le « Témoin » de l'incident.

L'investigation sur l'incident est de la responsabilité du déclarant. Une fois l'incident soumis pour validation à un responsable, le déclarant peut être sollicité à tout moment afin d'apporter des compléments d'information sur l'incident remonté (Cf. : causes, conséquences, description de l'incident, etc.). Par ailleurs, le déclarant peut être consulté pour la définition du plan d'actions associé à l'incident déclaré afin d'apporter des indications très opérationnelles et pertinentes dans sa mise en oeuvre.

La validation des incidents et des plans d'actions associés sont sous la responsabilité de chaque direction concernée.
La Direction du Contrôle Interne joue quant à elle un rôle de pilotage et d'animation du dispositif pour l'ensemble de l'établissement. Elle est la garante de la méthodologie de collecte des incidents et est en charge de :

- Déterminer les principes et les protocoles de collecte des incidents ;
- Identifier les acteurs du dispositif (déclarant, valideur, etc.) et de les former sur la méthodologie en vigueur ;
- Animer et coordonner le dispositif de collecte ;
- Etablir un reporting régulier vers la Direction Générale sur les incidents constatés et les mesures correctrices mises en place pour éradiquer l'incident et par la suite les actions préventives pour éviter que l'incident ne se produise à nouveau ;
- Coordonner le processus d'alertes pour les incidents importants, qui nécessitent d'être abordés lors d'un comité dédié ou bien remontés auprès d'une instance de direction, particulièrement

2.6.2 Reporting du dispositif de maîtrise des risques

Suite aux différents scandales qui ont touchés la sphère financière notamment, les régulateurs et les législateurs ont renforcé leur exigence en matière d'évaluation et d'information relatives au Contrôle Interne. Pour se faire, les Directions Générales et les Conseils d'Administration doivent avoir à leur disposition des outils de pilotage afin d'exercer pleinement leur responsabilité en matière de gestion des risques.
Une fois le dispositif de maîtrise mis en place, il convient d'élaborer des reportings sur les éventuelles défaillances de ce dernier. En effet, il est important d'apporter une attention toute particulière sur les faiblesses du dispositif car il peut s'agir de la perception d'une difficulté, potentielle ou avérée, à atteindre les objectifs de l'organisation ou d'une occasion de renforcer les chances de les atteindre.

L'organisation du reporting
Toutes les défaillances du dispositif de maîtrise des maîtrise qui affectent la capacité de l'organisation à élaborer et
mettre en oeuvre sa stratégie et à atteindre ses objectifs doivent faire l'objet d'une remontée à la bonne personne, c'est-à-dire celle qui est en mesure de prendre les décisions nécessaires à la résolution de cette défaillance. Ainsi, les défauts relevant des opérations courantes sont habituellement remontés au niveau hiérarchique immédiat, c'est-à-dire un chef de service. En fonction de la gravité et de la complexité de l'erreur, le responsable hiérarchique de l'opérationnel peut à son tour transmettre en amont ou transversalement l'information dans l'organisation de sorte qu'elle parvient à la personne ayant autorité pour la traiter correctement.

Dans le cadre où la défaillance porte atteinte à un objectif stratégique pour l'organisation ou bien à l'image de l'établissement, l'information doit être remontée au niveau le plus haut à savoir la Direction Générale et/ou le Conseil d'Administration. Pour se faire, il est nécessaire de définir et de mettre en place des protocoles afin de savoir comment l'information doit circuler au sein de l'organisation et à qui elle doit être adressée pour que la prise de décision soit efficace.

Vous êtes membre du Conseil d'Administration

› En qualité de membre du Conseil d'Administration, vous avez besoin d'être besoin d'être informé sur le niveau de risque auquel est soumis votre organisation et sur le risques susceptibles de compromettre l'atteinte de vos objectifs stratégiques. Pour se faire, vous avez besoin d'indicateurs vous permettant de mesurer le couple "Rendement-risque".

Vous êtes une Direction Générale

› En qualité de chef d'établissement, vous avez besoin d'être informé des manquements importants aux politiques et procédures en vigueurs. Vous avez également besoin d'informations sur les questions pouvant avoir un impact financier important ou des conséquenses stratégiques qui seraient susceptible de nuire à la réputation de l'organisation.

Vous êtes une Direction Opérationnelle

› En qualité de chef de service, vous devez être informés des défaillances du dispositif de maîtrise des risques et des contrôles qui affectuent votre unité. Il peut s'agir par exemple d'un manque de formation d'un collaborateur sur une tâche donnée, un dysfonctionnement sur un processus opérationnel.

La mise en place d'indicateurs
Pour garantir un suivi efficace des systèmes de Contrôle Interne et de gestion des risques, il est préconisé de définir et de mettre en place des indicateurs clés de performance relatif au dispositif. Ces indicateurs vont vous permettre de mesurer :

- L'efficacité des plans d'actions et l'atteinte des objectifs – KPI (Key Performance Indicator) ;
- L'évolution des risques pouvant impacter l'atteinte des objectifs – KRI (Key Risk Indicator).

➤ **Key Performance Indicator :**
La mise en place de ces indicateurs va permettre de mesurer le niveau d'atteinte d'un objectif stratégique et donc de juger de la performance d'un processus clé. Véritable outil d'aide à la décision, son but est d'évaluer l'évolution d'un élément clé et de la comparer aux objectifs pour lequel il a été créé.

Compte tenu du caractère stratégique que revêt cet indicateur, il est généralement défini par la direction et mis en perspective avec les objectifs organisationnels.

L'objectif d'un KPI peut être :

- L'évaluation d'un plan d'action ;
- L'évolution d'une action ;
- La communication d'une action ;
- Etc.

D'autre part, un KPI doit être :

- **Valide** – C'est-à-dire que l'indicateur doit porter sur une information utile et exploitable par tous ;
- **Mesurable et évaluable** dans le temps – C'est-à-dire que les données doivent être disponibles, traçables pour permettre une mise à jour périodique ;
- **Réaliste** – C'est-à-dire que l'indicateur doit mesurer un objectif réaliste et donc atteignable ;
- **Spécifique** – C'est-à-dire que l'indicateur ne doit traiter qu'une seule information au risque de s'éparpiller et de rencontrer des difficultés pour ensuite pouvoir le mesurer.

➤ **Key Risk Indicator :**
Ces indicateurs permettent de suivre au plus près l'évolution des risques en distinguant les risques dits « Critiques » et les risques « Clés ». Ils donnent une mesure régulière de l'exposition de l'établissement aux risques qu'il l'entoure.

Quelques principes :
- Le KRI est une donnée objective, quantifiable, facilement reproductible, documentée et auditable ;
- Le KRI peut être lié à un ou plusieurs type(s) de risque ;
- Un indicateur de risque est qualifié de « Clé » dès lors qu'il identifie :
  - Une ou plusieurs zones de risque importante(s) ;
  - Ou des zones bien maîtrisées sur lesquelles une défaillance du Dispositif de Maîtrise des Risques (DMR) ferait porter un risque brut majeur.

La mise en place de KRI répond à plusieurs objectifs :

- Alerter la Direction Générale et le management de l'établissement sur les activités porteuses de risques grâce notamment à :
  - Une évaluation régulière des améliorations ou des détériorations du profil de risques ;
  - Une évaluation régulière de l'environnement de prévention et de contrôle.
- Anticiper les activités porteuses de risques et ainsi pouvoir réagir de manière plus appropriée face aux menaces qui pèsent sur l'établissement (Mise en place de plans d'actions additionnels, etc.).

2.7 La gestion des conséquences d'un risque avéré – Exemple de la réclamation d'un bénéficiaire

2.7.1 Les risques relatifs à une réclamation

Le mécontentement d'un bénéficiaire se manifeste en général par la remontée d'une réclamation auprès de la direction commerciale ou bien auprès du service des réclamations quand celui-ci existe. Une réclamation peut porter sur :

- Un délai de traitement (absence ou retard) ;
- Un problème relationnel, de communication ou de conseil ;

- Une politique tarifaire ;
- Un traitement non conforme ;
- La contestation d'une décision de l'établissement suite à la réclamation.

Cette démarche envoie un signal fort à l'entreprise pour lui signifier que le service ou le produit proposé n'est pas à la hauteur des attentes du bénéficiaire. Cette insatisfaction fait encourir plusieurs risques à l'établissement, dont les principaux sont les suivants :

Risque de réputation : Une réclamation mal ou pas traitée peut avoir des conséquences lourdes pour l'entreprise et notamment au niveau de l'atteinte de sa réputation. Ainsi, la contagion médiatique peut se trouver accentuée du fait de la judiciarisation de la société (Ex. : Gestion du contentieux, action de groupe), la montée de l'opinion publique (Ex. : Association de défense des consommateurs) et l'avènement des réseaux sociaux (Ex. : Message de mécontentement sur la page Facebook ou Twitter).

Risque de non-conformité : Il s'agit ici pour l'établissement de prévenir le contentieux. En effet, le traitement d'un contentieux engendre des coûts qui peuvent être non négligeables (Cf. : frais des procès, paiement de dommages, etc.), et peut avoir des répercussions malheureuses sur l'image et la réputation de l'établissement. D'autre part, certaines entités vantent au travers de la publicité la qualité de leurs produits ou services et le risque de non-conformité devient avéré dès lors qu'il y a un décalage entre la promesse attendue et le résultat obtenu.

Risque de perte de chiffre d'affaires (uniquement pour les services publics marchands) : Il faut savoir qu'un bénéficiaire satisfait le dit à 3 personnes. En revanche, un bénéficiaire mécontent le dit à 10 personnes. D'autre part, il est plus facile et moins couteux de fidéliser des bénéficiaires que d'en conquérir de nouveaux d'où l'importance d'apporter une attention particulière aux réclamations mais également sur la manière dont le réclamant a perçu le traitement de sa demande afin que l'entité puisse d'une part, optimiser le processus de traitement des réclamations et d'autre part, améliorer le service ou le produit proposé.

2.7.2 Le traitement d'une réclamation

Comme nous venons de le voir dans le précédent paragraphe, l'absence ou le retard de traitement d'une réclamation peut engendrer des risques qu'il convient de contenir rapidement. Aussi, il convient de disposer d'un système de traitement des réclamations éprouvé et efficace afin de proposer le meilleur niveau de qualité de service et ainsi satisfaire la demande du bénéficiaire.

Pour cela, attardons nous quelques instants sur les attentes d'un bénéficiaire suite à une réclamation. Il s'attend à :

- Comprendre, être compris et surtout être entendu ;
- Etre orienté vers le bon interlocuteur ;
- Etre assuré de la bonne prise en compte de sa réclamation ;
- Etre assuré que son dossier sera réexaminé ;
- Etre informé régulièrement des suites données à sa réclamation ;
- Obtenir une solution adaptée avec des délais de réponse et/ou de résolution rapides ;
- Ne pas avoir à faire deux fois la même réclamation.

Avec le développement du tout digital et des outils de communication, le consommateur du 21ème siècle est de plus en plus exigeant, informé des obligations qui régissent les entités publiques et conscient de ses droits. Il est donc tout naturel pour lui de solliciter une aide auprès d'un service en cas de désaccord ou tout simplement pour obtenir des compléments d'informations.

> Le bénéficiaire qui exprime son mécontentement vous offre la possibilité de **renouer le dialogue**, de **regagner sa confiance** et de **vous améliorer**.

Il devient donc nécessaire de traiter chaque réclamation avec comme objectif de trouver une solution adaptée aux besoins du bénéficiaire. Les enjeux pour les établissements sont multiples :

- Canaliser l'expression du mécontentement et le traiter prioritairement ;
- Résoudre les conflits, prévenir leur aggravation et limiter leurs conséquences juridiques et financières ;

- Apporter systématiquement des explications claires et des solutions aux bénéficiaires ;
- Identifier le dysfonctionnement pour mettre en oeuvre les actions d'amélioration adéquates ;
- Maintenir une bonne image de l'établissement.

Une déclaration bien traitée, c'est une **opportunité** de **satisfaire** et de **fidéliser** les bénéficiaires de vos services

Le bon traitement d'une réclamation peut se résumer de la manière suivante :

Information et accès de la clientèle au système de traitement des réclamations

- Informer les clients dans un langage claire et compréhensible sur les modalités et les délais de traitement des réclamations et sur l'existence d'une charte/protocole de médiation.
- Rendre l'information accessible à l'ensemble de la clientèle : affichage aux lieu d'accueil et sur le site internet
- Accuser réception des réclamations dans les délais
- Tenir le client informé du déroulement du traitement de sa réclamation
- Préciser les voies de recours en cas de rejet ou refus de la réclamation, préciser notamment les coordonnées du médiateur
- Éviter toute confusion entre les services interne de l'organisme et le dispositif de médiation indépendante

Organisation du traitements des réclamations

- Mettre en place les moyens et les procédures permettant d'identifier les réclamations (courriers, appels téléphoniques et courriels) et de définir le traitement de celles-ci
- Former le personnel concerné
- Mettre en place une organisation appropriée pourle traitement des réclamations
- Formaliser cette organisation dans une (des) procédure (s) de traitement des réclamations de la clientèle communiquée à l'ensemble des collaborateurs concernés

Suivi, contrôle du traitement des réclamations et la prise en compte des manquements ou mauvaises pratiques identifiés à travers les réclations

- Mettre en place un suivi des réclamations et d'en effectuer une restitution aux services / personnes concernés de l'entité
- Indentifié les manquements et mauvaises pratiques en matière de commercialisation et de protection de la clientèle afin de mettre en œuvre les actions correctives
- Mettre en place les moyens et les procédures nécessaires pour assurer un contrôle interne adapté sur l'information délivrée, l'organisation et la qualité du traitements des réclamations
- Prendre en compte et contrôler, au titre du contrôle interne, les risques subis par la clientèle que pourraient causer les manquements et/ou atteintes aux règles de protection de la clientèle, identifiés au travers des réclamations
- Garder la trace des contrôles effectués

Exemple de circuit de traitement d'une réclamation sur 3 niveaux :

Niveau 1 : Le bénéficiaire s'adresse en premier lieu à un interlocuteur habituel (Ex. : une entité commerciale) ;

Niveau 2 : Le bénéficiaire s'adresse à un interlocuteur inhabituel (Ex. : Service des réclamations, Direction Générale, Présidence, Association des consommateurs, CNIL, etc.) ;

Niveau 3 : Le bénéficiaire s'adresse à un médiateur lorsque toutes les voies de recours au sein de l'établissement sont épuisées.

2 Les pré-requis permettant la mise en place du Contrôle Interne

Avant de se lancer dans un projet de mise en place d'un dispositif de Contrôle Interne et de maîtrise des risques, il convient de s'assurer que les éléments fondamentaux à la réussite et au bon dimensionnement de la démarche ont bien été identifiés et communiqués et compris par l'ensemble des parties prenantes. Il s'agit pour cela de :

- Décrire et présenter formellement les attentes de la Direction. Cela se traduit par la définition des objectifs stratégiques et opérationnels que l'exécutif souhaite atteindre, les moyens qu'il met en oeuvre pour y arriver et enfin les bénéfices qu'il souhaite tirer de cette démarche ;
- Désigner le ou les personnes qui assureront le rôle de sponsor de la démarche auprès de la Direction Générale et des directions opérationnelles et supports ;
- Définir les contours des activités opérationnelles et fonctionnelles qui rentrent dans les travaux ;
- Identifier et dimensionner les ressources utiles pour une mise en place rapide et efficace.

La check-list suivante propose d'avoir un aperçu synthétique, par thématique, des pré-requis nécessaires à la mise en place d'un dispositif de Contrôle interne.

Cette check-list s'organise autour des grands thèmes suivants :

- Vision stratégique du dispositif
- Implication de la Gouvernance
- Ressources internes / budget
- Méthodologie
- Système d'information

Répondrez à ces questions simples et déterminez immédiatement votre niveau de préparation.

VISION STRATÉGIQUE

Si l'objectif principal d'un dispositif de contrôle interne est de réduire l'exposition aux risques, il n'en demeure pas moins un véritable outil permettant d'agir sur tous les leviers d'amélioration des performances de l'entreprise et doit être appréhendé comme tel.

Avez-vous un comité d'audit ?
☐ Oui
☐ Non

Avez-vous formalisé votre dispositif au travers de chartes approuvées par le comité d'audit ?
☐ Oui
☐ Non

Votre Contrôle Interne est-il identifié comme un vecteur de performance ?
☐ Oui
☐ Non

Avez-vous construit une carte stratégique pour votre organisation ?
☐ Oui
☐ Non

Avez-vous une cartographie de vos risques ?
☐ Oui
☐ Non

Votre Contrôle Interne est-il identifié comme un vecteur d'amélioration permanente ?
☐ Oui
☐ Non

Avez-vous insufflé une culture risque au sein de votre établissement ?
☐ Oui
☐ Non

IMPLICATION DE LA GOUVERNANCE

Pour qu'elle fédère autour d'elle l'ensemble des acteurs internes et externes, la démarche doit être promue au plus haut niveau de l'organisme public considéré. Ainsi les directeurs généraux apparaissent comme les principaux soutiens de la démarche pour encourager la démarche de contrôle interne et instaurer une véritable culture de la gestion des risques au sein de leur administration.

Est-ce que la Direction Générale et le conseil d'administration sont impliqués dans le dispositif de Contrôle Interne ?
- ☐ Oui
- ☐ Non

Les rapports du Contrôle Interne sont-ils communiqués aux administrateurs ?
- ☐ Oui
- ☐ Non

Les rapports du Contrôle Interne sont-ils communiqués à la Direction Générale ?
- ☐ Oui
- ☐ Non

Le comité d'audit se réunit-il à fréquence régulière et plus d'une fois par an ?
- ☐ Oui
- ☐ Non

Le Contrôle Interne dépend de la direction financière
- ☐ Oui
- ☐ Non

Le Contrôle Interne dépend de la Direction Générale
- ☐ Oui
- ☐ Non

RESSOURCES INTERNES / BUDGET

La mise en place d'un dispositif de contrôle interne engage nécessairement des moyens humains et financiers.

Avez-vous une équipe permanente de Contrôle Interne ?
- ☐ Oui
- ☐ Non

Est-elle formée régulièrement, chaque année ?
- ☐ Oui
- ☐ Non

Le programme de contrôle peut-il être mené à bien ?
- ☐ Oui
- ☐ Non

Avez-vous les moyens de faire appel à des auditeurs externes ?
- ☐ Oui
- ☐ Non

MÉTHODOLOGIE

Le dispositif de contrôle interne doit s'appuyer sur une méthodologie clairement définie et partagée auprès des différents acteurs.

Les contrôles sont menés en tenant compte de la cartographie des risques
- ☐ Oui
- ☐ Non

Les contrôles suivent une méthodologie définie par le comité d'audit ?
- ☐ Oui
- ☐ Non

Le rapport est normalisé ?
- ☐ Oui
- ☐ Non

Les préconisations des précédents rapports sont revues ?
- ☐ Oui
- ☐ Non

Avez-vous formalisé et testé un plan de continuité d'activité (PCA) ?
- ☐ Oui
- ☐ Non

SYSTÈME D'INFORMATION

Les conséquences d'un mauvais fonctionnement du SI sur les risques d'une entité sont évidentes et de plus en plus nombreuses, tant le rôle joué par les SI dans le comportement d'une organisation est devenu important.

Avez-vous confiance en votre système d'information (sécurité formelle) ?
- ☐ Oui
- ☐ Non

Des traitements de gestion sont-ils faits en dehors de votre SI ?
- ☐ Oui
- ☐ Non

Avez-vous fait des tests de fraudes ou d'intrusions ?
- ☐ Oui
- ☐ Non

3 Les spécificités du Contrôle Interne par type d'organisation

Le dispositif de contrôle doit s'appuyer sur une analyse de l'environnement et des caractéristiques (métiers, effectifs, statuts, localisation, etc.) propres de la structure dans laquelle il est déployé.
Les problématiques peuvent donc varier d'un organisme public à l'autre, et les risques rencontrés, bien que pouvant être de même nature, requièrent des stratégies de traitement qui peuvent être différentes.
La cartographie suivante propose une classification des différents types de services publics, chacun d'entre eux étant illustrés par un retour d'expérience.

Service Public en France

Fonctions Régaliennes : Il s'agit des fonctions de souveraineté de l'État. Elles sont entièrement financées par impôt et assurées par des administrations publiques.

Services Publics non marchands : il s'agit des services pour l'essentiel gratuits et financés principalement par impôt (ou les cotisations obligatoires). Les établissements relèvent du droit administratif, mais ces services associent aussi des organismes privés (sous contrat) et des associations.

Services Publics marchands : il s'agit de services financés principalement par une activité commerciale

1. RETOUR D'EXPERIENCE : CAS DE L'INSTITUT NATIONAL DE POLYTECHNIQUE DE GRENOBLE

1.1 Présentation générale de l'INPG

L'Institut National Polytechnique de Grenoble est un EPSCP (Etablissement Public à Caractère Scientifique, Culturel et Professionnel) et se trouve sous l'autorité du ministère de l'enseignement supérieur et de la recherche.
Plébiscité par les étudiants, Grenoble INP occupe la tête du classement des établissements les plus actifs en matière d'innovation et de recherche et est reconnu pour son excellence académique.

Les activités de Grenoble INP se répartissent selon deux grands axes, à savoir :

- La formation de 5000 étudiants ingénieurs par an au travers de 6 écoles d'ingénieurs ;
- La recherche avec 36 grands laboratoires spécialisés dans les sciences de l'ingénieur. Ils préparent les technologies du futur dans six domaines clés : Energie, Environnement, Information et communication, Matériaux, Micro et nanotechnologies et les Systèmes de production.

Grenoble INP est dirigé par un administrateur général, élu par les communautés scientifiques et administratives de l'établissement pour une durée de 4 ans. Son rôle est de prendre en charge la conduite des opérations et de définir la stratégie de l'établissement afin de renforcer la visibilité de sa position nationale et internationale. Luimême et les membres de son équipe sont généralement issus du monde de l'enseignement et de la recherche.
Son équipe est également composée d'un Directeur Général des Services (non élu), en charge de la gestion opérationnelle de l'établissement, de la veille et du contrôle juridique, de l'administration et de l'encadrement.
Alain Scordel est Directeur Financier de Grenoble INP depuis 4 ans. Il dépend directement du Directeur Général des Services et occupe un rôle d'ordonnateur au sein de l'établissement. L'agent comptable assure la tenue de la comptabilité et la production du compte financier de l'établissement. En sus de ses fonctions, Alain Scordel a sous sa responsabilité les fonctions de Contrôle de gestion et de Contrôle Interne. Il est prévu que le service Achats de l'INP Grenoble soit prochainement rattaché à la Direction Financière.

1.2 Nécessité et ébauche du Contrôle Interne

La loi sur l'autonomie des universités constitue un des déclencheurs pour la mise en place du Contrôle Interne au sein de Grenoble INP.
Fin 2011, l'équipe dirigeante en place impulse la mise en place d'un dispositif de Contrôle Interne. En 2012, une première cartographie des risques selon une approche « Top-Down » est réalisée et couvre la totalité des processus de l'entité, comprenant au total une cinquantaine de risques. Sur la même période, un système de gouvernance est mis en place et un Directeur du Contrôle Interne est recruté.
Afin de faciliter l'appropriation du dispositif de Contrôle Interne et favoriser la diffusion d'une culture risque au sein du personnel scientifique et administratif, plusieurs initiatives voient le jour :

- Tout d'abord, la terminologie « Contrôle Interne » est renommée « Processus d'amélioration continue » ;

- Par la suite, la direction choisit d'initier la démarche en se focalisant en priorité sur les risques issus des processus financiers et comptables, car la population concernée est déjà sensibilisée à la notion de Contrôle Interne et de maîtrise des risques.

1.3 Modalités de la mise en place effective

Plusieurs difficultés ont affecté la mise en place/ la pérennisation du dispositif :

- Des mouvements dans l'équipe de direction et notamment du responsable du Contrôle Interne ont ralenti d'une part, le processus de mise en oeuvre du dispositif de Contrôle Interne au sein des différentes activités de l'établissement et, d'autre part, ont rendu plus difficile l'appropriation de la démarche et la diffusion de la culture risque à tous les niveaux de l'organisation.

- Afin d'assurer néanmoins une continuité dans les travaux, il a été décidé de basculer le Contrôle Interne sous l'autorité de la Direction financière, véritable sponsor de la démarche aujourd'hui.

- La mise en place d'une nouvelle équipe dirigeante en 2012 a également contribué à modifier la mise en place du dispositif : à cette occasion, la vision stratégique de l'établissement a été revue par la nouvelle équipe et les objectifs de performance ont été redéfinis. Le Contrôle Interne se reposant sur ces deux éléments pour définir sa propre stratégie et ses objectifs, il a été très difficile de progresser pendant cette période.

- Les campagnes de consultation réalisées auprès des différentes équipes de l'établissement ont permis de révéler un questionnement des professionnels de recherche et de formation sur les enjeux et les objectifs du Contrôle Interne. Fort de ce constat, cela a permis d'ajuster les interviews et le discours afin de commencer à sensibiliser le personnel de Grenoble INP sur les démarches de Contrôle Interne et de r éaliser un bilan d'avancement global.

- Une initiative d'appropriation du dispositif de Contrôle Interne au niveau local est d'ailleurs à noter puisque l'école PAGORA dédiée aux formations techniques de la papeterie a mis en place une démarche Qualité qui s'inscrit parfaitement dans la politique que souhaite donner l'établissement en matière de prévention et de maîtrise des risques.

A ce jour, on peut dire que la démarche est en veille et qu'il convient d'envisager d'y donner une nouvelle impulsion.
Le départ du responsable en charge de piloter l'approche a été l'une des difficultés majeures expliquant cette situation. Le fait de rattacher le Contrôle Interne à la Direction Financière peut constituer une opportunité pour relancer le projet et le faire aboutir.

1.4 Nécessité et ébauche du Contrôle Interne

L'arrivée d'un nouveau responsable du Contrôle Interne, les efforts de sensibilisation menés par le Directeur Général des Services et le Directeur financier auprès de la Présidence devront permettre de garantir un fort niveau d'investissement sur le sujet dans les mois à venir et ce malgré le départ prochain de l'un des principaux sponsors du Contrôle Interne de Grenoble INP, le DGS.
De plus, les travaux futurs de mise en conformité avec la nouvelle réglementation GBCP sont perçus comme un véritable levier de performance et d'optimisation des processus pour Grenoble INP et devraient favoriser une généralisation du dispositif de Contrôle Interne au sein de l'établissement.
Ce levier devra être exploité au maximum, notamment à travers un véritable plan d'information et de communication auprès des responsables opérationnels des métiers de la recherche et de la formation.
Grenoble INP est aujourd'hui confronté aux défis de la concurrence internationale et de la concentration progressive des établissements d'enseignement supérieur. Face à ces défis, il est devenu nécessaire de garantir un haut niveau de contrôle des processus financiers et de disposer d'un dispositif de Contrôle Interne éprouvé et efficace permettant de tendre vers la résilience.

FICHE TECHNIQUE DE L'ENTITÉ PUBLIQUE
GRENOBLE INP
Institut National Polytechnique de Grenoble

Alain SCORDEL – Directeur Administratif et Financier de Grenoble INP
Grenoble INP a le statut de Grand Etablissement. À ce titre, il est un établissement public à caractère scientifique, culturel et professionnel (EPCSCP). Il y a 6 écoles d'ingénieur, dont 5 qui sont situées sur Grenoble et une à Valence. Il y a 21 laboratoires en France et 10 à l'étranger.
Grenoble INP réalise deux missions fondamentales, à savoir :

- La formation d'ingénieurs et de docteurs adaptée aux enjeux d'aujourd'hui ;

- La recherche de haut niveau et une valorisation efficace dans les domaines scientifiques contribuant aux enjeux sociétaux et défis industriels : les micronanotechnologies, l'énergie, la société numérique, l'environnement et l'industrie; mondialisation et innovations, qui incluent les missions d'orientation et d'insertion professionnelle, de diffusion de la culture scientifique, de coopération interna-

tionale, de participation à la construction de l'espace européen.

CHIFFRES CLÉS :

Pour la recherche :
- 1 400 personnes

2. RETOUR D'EXPERIENCE : CAS DE LA SNCF

2.1 Un dispositif de Contrôle Interne est-il en place au sein de votre établissement ?

A. Quelles en sont les missions ?
En 2009, à l'initiative de la Direction Générale de la SNCF, une mission d'audit a été lancée pour apprécier la qualité des dispositifs de Contrôle Interne au sein de la SNCF.

Cet audit a été mené au sein des différentes structures matricielles de l'entreprise, croisant le découpage géographique et l'organisation par branche d'activités.

Il s'est avéré que de nombreuses démarches existaient, mais qu'elles n'étaient pas nécessairement coordonnées et que les organisations présentaient des insuffisances notables :

- La maîtrise du Contrôle Interne des processus était apparue globalement médiocre,
- Des différences sensibles de maîtrise existaient au sein d'un même processus,
- Le référentiel AMF n'était pas couvert de façon exhaustive

A partir de ce constat, il a été décidé de mettre en place une véritable démarche de Contrôle Interne en s'appuyant sur la direction de l'audit et des risques (DAR) et la direction financière.
La DAR répond hiérarchiquement à la Direction Générale et fonctionnellement au Comité d'audit.
Elle exerce trois missions principales :

- L'animation de la démarche risques et l'identification des risques majeurs de l'entreprise ;
- Le développement du Contrôle Interne ;
- La réalisation de missions d'audit.

L'identification des risques majeurs
En complément des initiatives de Contrôle Interne, des actions d'identification des risques majeurs de l'entreprise ont conduit à dresser une cartographie des risques clefs qui sont de nature « à empêcher les dirigeants de dormir ».

Cette approche est menée par interviews des principaux dirigeants sur la manière dont ils apprécient les risques :

- Niveau de risque combinant l'impact et sa probabilité de survenance,
- Niveau de maîtrise du risque.

Elle s'enrichit également d'une remontée des principaux risques émanant des cartographies des branches et domaines, qui sont analysés et exploités par la DAR pour en extraire des thématiques communes.

Cette démarche est réalisée selon une approche croisée top down et bottom-up et fait l'objet d'une actualisation annuelle.

L'animation du Contrôle Interne
A la suite de l'audit de 2009, a été engagée une démarche d'identification des risques majeurs concernant les 14 processus comptables et financiers du guide d'application du cadre de référence de l'AMF.

La démarche a d'emblée écarté une approche complète incluant les risques opérationnels de l'entreprise, car jugée trop lourde et plus difficilement appropriable par les acteurs opérationnels. L'analyse des processus et risques opérationnels se fera dans un deuxième temps.

La mise en place du Contrôle Interne a été pilotée par la DAR et la Direction Financière et s'est appuyée sur les branches au sein desquelles ont été mis en place des correspondants de Contrôle Interne.

Elle s'est déroulée au cours des années 2011 à 2013, selon les différentes étapes suivantes :

- En 2011, définition des principes, méthodes et outils, constitution du réseau des correspondants.
- En 2012, premier test complet de la démarche sur le processus « Paie » avec description du processus, identification d'une trentaine de risques associés et détermination de points de contrôle clés.
- Premières auto-évaluations de la maîtrise des points de contrôle clés des processus paie, achats et immobilisations, suivant une grille d'évaluation à quatre niveaux.
- Puis, à partir de 2013, généralisation à l'ensemble des autres processus du référentiel AMF, à l'aide d'un outil de Contrôle Interne : ENABLON. Ce produit a permis de faciliter le déploiement des campagnes, le partage des bonnes pratiques et le suivi des plans d'actions, non seulement dans les branches, mais égale-

ment dans les filiales. Geodis en était déjà un premier utilisateur.

La réalisation des missions d'audit
La DAR réalise chaque année des missions d'audit sur des points clefs du Contrôle Interne arrêtées au sein d'un plan d'audit.

Les conclusions de ces audits font l'objet de différents reportings : auprès du Comité Exécutif, auprès du comité d'audit et auprès de la Mission de Contrôle Economique et Financier des Transports (organe de surveillance de la SNCF rattaché à Bercy).

B. Sur quel schéma de gouvernance repose t'il ?
La DAR rattachée au Comité exécutif est responsable de la démarche en lien avec la direction Financière. La DAR compte une cinquantaine de personnes réparties autour des 3 missions présentées précédemment.

Elle s'appuie sur un réseau de contrôleurs internes établis au sein de chaque branche. Ces derniers sont réunis en séminaire 3 à 4 fois par an.

Tous utilisent la même méthode de travail et le même outil de Contrôle Interne ENABLON.

Chaque structure de Contrôle Interne travaille en étroite relation avec chacune des directions financières de branche.

C. Quels sont les acteurs et les parties prenantes du dispositif ?
La Direction Générale et les membres du Comité Exécutif sont impliqués dans la démarche. Il s'avère que grâce à l'approche progressive de la mise en place, l'appropriation du sujet par les responsables opérationnels et notamment les responsables de branches et d'établissements locaux a été effective.

2.2 Dans quelle mesure, la mise en place de ce dispositif vous permet-il d'atteindre les objectifs suivants :

• Sécuriser vos activités ?

A ce jour l'approche n'a pas encore été déployée sur les processus opérationnels, il est toutefois à noter que les principaux de ces processus, et notamment la sécurité des circulations ferroviaires relèvent d'une approche très organisée et conforme aux principes de contrôle interne mais utilisant des outils différents.

• Identifier les zones de vulnérabilité ?
Le déploiement des 14 processus comptables et financiers du référentiel de l'AMF a permis de cerner les zones de vulnérabilité comme par exemple le respect des règles de séparation des tâches et de mettre en oeuvre les plans d'action appropriés.
• Améliorer la qualité ?
Il est encore trop tôt pour bien en mesurer l'impact mais cette démarche est vertueuse car elle permet aux

2.3 Avez-vous déjà observé des premiers résultats ? Si oui, dans quels domaines ?

La démarche de Contrôle Interne est maintenant bien intégrée dans l'entreprise et ne fait pas l'objet de remise en cause par les responsables. Elle a permis notamment de rationaliser les méthodes de travail au sein des 14 processus de l'AMF

2.4 Quels sont les chantiers prioritaires de votre organisation dans les années à venir concernant la gestion des risques et le Contrôle Interne ?

La démarche est maintenant complètement opérationnelle autour des 14 processus comptables et financiers recensés par l'AMF.
Il convient de la déployer auprès des processus opérationnels de l'entreprise afin de mieux se coordonner avec les autres risques de l'entreprise et de fortifier la cartographie des risques majeurs

2.5 Quelles sont les actions que vous avez prises ou prévues de prendre pour répondre au décret 2012-1246 du 7 novembre 2012 relatif à la Gestion Budgétaire et Comptable Publique (GBCP) ?

L'entreprise n'est pas concernée par le GBCP. Elle produit ses résultats annuels selon les mêmes règles que les autres entreprises.

2.6 Quelles sont les difficultés majeures que vous rencontrez ou pensez rencontrer concernant vos projets relatifs à la gestion des risques et au Contrôle Interne ? Le déploiement aux autres risques opérationnels de l'entreprise

Le déploiement aux autres risques opérationnels de l'entreprise constitue le chantier à mettre en oeuvre.
Deux difficultés peuvent apparaître :

• L'ampleur du sujet qui consistera à analyser les grands processus opérationnels de l'entreprise,

• L'acceptation par les opérationnels.

FICHE TECHNIQUE DE L'ENTITÉ PUBLIQUE

SNCF

Raymond MARFAING – Directeur adjoint – Direction de l'Audit et des Risques

La SNCF est un groupe public proposant de multiples services de transport. Elle a le statut d'établissement public à caractère industriel et commercial (EPIC). Le groupe se structure autour de 5 activités principales :

- **SNCF Proximité** - Service de transport public de voyageurs urbain, périurbain, régional, interrégional
- **SNCF Voyages** - Transport de voyageurs longue distance et distribution
- **Gares & Connexions** - Gestion et développement des gares
- **SNCF Geodis** - Transport et logistique de marchandises
- **SNCF Infra** - Gestion, exploitation, maintenance et ingénierie d'infrastructures à dominante ferroviaire

Les activités du groupe SNCF couvrent en 2013 120 pays et le posent en l'un des leaders mondiaux de la mobilité des personnes et du transport et logistique de marchandises.

Chiffres clés 2013 :

➢ **Groupe SNCF**
- 32,2 Mds d'€ de chiffre d'affaire
- 2,8 Mds d'€ de marge opérationnelle
- 250 000 salariés
- 2,2 Mds d'€ d'investissements

➢ **SNCF Proximité**
- 11,9 Mds d'€ de chiffre d'affaire
- 10 Millions de voyageurs par jour
- 655 Millions d'€ de marge opérationnelle
- +53% de hausse du trafic TER depuis 2002

➢ **SNCF Voyages**
- 6,8 Mds d'€ de chiffre d'affaire
- 126,9 Millions de voyageurs transportés sur l'année 2013
- Voyages-sncf.com est la première agence de voyages en ligne en France
- Plus de 2 Mds de clients des lignes à grande vitesse depuis 1981

➢ **Gares & Connexions**
- 1,2 Mds d'€ de chiffre d'affaire
- 2 Mds de voyageurs transitent chaque année par les gares SNCF
- 3029 gares et haltes de voyageurs en France en 2013, dont 383 sur le réseau transilien
- 2 Millions de mètres carrés d'espaces d'accueil et de vente

➢ **SNCF Geodis**
- 1er opérateur français de transport de marchandises
- 4ème opérateur européen
- 46% du chiffre d'affaire réalisé à l'international

➢ **SNCF Infra**
- 30 000 km de réseau maintenu et surveillé 24 heures /24
- 15 500 trains gérés au quotidien par la Direction de la circulation ferroviaire
- 1300 chantiers majeurs en 2013

3. RETOUR D'EXPERIENCE : CAS D'UN ÉTABLISSEMENT POUR PERSONNES ÂGÉES SUISSE

3.1 Présentation

James Wampfler est directeur de deux établissements pour personnes âgées (EMS) de moins d'une centaine de lits chacun (55 et 71) situés en Ville de Genève. Ces derniers s'intègrent dans une Fondation. La situation entre les deux EMS est quelque peu différente.

3.2 Un dispositif de contrôle interne organisé et formalisé est-il en place au sein de votre établissement ?

Notre système de contrôle interne (SCI) existe depuis plusieurs années au sein des deux entités. L'historique, le contexte, l'état d'esprit et les modalités de fonctionnement n'y sont pas forcément identiques sur tous les plans.

La préoccupation originelle relevait de la Qualité avec principalement la volonté de passer de classeurs papier à des classeurs informatiques. Cette évolution prenait tout son sens pour accéder en temps réel aux informations à jour et utiles au fonctionnement : processus, procédures, protocoles divers par exemple en cas de disparition d'un résidant, organigramme, cahiers des charges, etc.

Dans un second temps avec les exigences, d'une part du Canton de Genève comme subventionneur, d'autre part de nature légale et des attentes de notre réviseur aux comptes, nous avons mis progressivement en place un SCI de natures comptable et financière puis plus opérationnel.

Enfin le cadre légal évolue constamment avec en guise d'exemple des exigences nouvelles en matière d'accès à l'information par des tiers ; dans ce cadre une réflexion globale en la matière a dû avoir lieu.

Il est intéressant de relever à ce propos que la Qualité avec l'ajout des risques tend à se

rapprocher du contrôle interne (CI). Cette évolution s'est aussi faite au niveau de l'application informatique - OPTIMISO - qui nous accompagne depuis longtemps.

3.3 Dans quelle mesure, la mise en place de ce dispositif vous permet-il d'atteindre les objectifs suivants : sécuriser vos activités ; identifier les zones de vulnérabilité ; améliorer la qualité ; aider au pilotage stratégique ?

Ces objectifs peuvent être atteints par le CI et la liste ci-avant reflète bien leur ordre d'importance. Toutefois d'autres éléments y concourent également comme la formation et la motivation des collaborateurs.

Dans ce cadre il est opportun de relever que la démarche de mise en place de la documentation peut être, voire même doit être, plus participative. En revanche elle sera plus directive pour ce qui concerne les risques et les contrôles.

Quant à la stratégie d'implémentation de la documentation elle a aussi toute sa logique. En l'espèce il semble faire sens de commencer par les activités qui touchent plusieurs secteurs, puis celles qui ne relèvent que d'un secteur respectivement quelques personnes, pour terminer par ce qui concerne qu'une personne.

3.4 Avez-vous déjà observé des premiers résultats ? Si oui, dans quels domaines ?

Les résultats s'observent à plusieurs niveaux et dans plusieurs domaines. C'est toute une série d'éléments qui forment un tout :

- Le Conseil de la Fondation dispose de toutes les informations utiles, notamment sur les risques.
- Les collaborateurs ont accès à toutes les informations concernant le CI avec y compris les risques.
- La dépendance au papier, avec tous ses inconvénients, a disparu.
- Le CI est intégré aux activités et est une pièce parmi d'autres de notre système de gestion.
- Nous visons une sorte d'idéal avec la mise en place d'un Intranet permettant d'une part d'avoir une vision globale et, d'autre part « forcer » à n'utiliser qu'une seule porte d'entrée. OPTIMISO n'est en effet qu'une des applications nécessaires au fonctionnement d'un EMS.

3.5 Quelles sont les difficultés majeures que vous rencontrez ou pensez rencontrer concernant vos projets relatifs à la gestion des risques et au contrôle interne ?

Les difficultés, mais qui sont en soi un défi, sont les suivantes en regard d'un dispositif qui est bien rodé :

- Maintenir intuition et pragmatisme.
- Concilier souplesse et rigidité.
- Rester dans le bon sens et non pas que les collaborateurs se réfugient derrière les procédures.
- Passer progressivement d'une vision en quelque sorte statique dans l'optique d'une certification qualité annuelle à un dispositif dynamique. Autrement dit comme l'exprime souvent Benedikt Cordt-Møller il s'agit de passer de la photo au film.
- Continuer à disposer d'une application informatique qui réponde constamment à nos besoins en matière de Qualité et de CI.
- Arriver à une culture partagée du CI qui repose principalement sur une totale ouverture, c'est-à-dire ne rien cacher.
- Trouver la bonne granularité tant sous l'angle du dispositif dans son entier que par exemple sur les contrôles, et donc in fine sur leur nombre.
- Limiter le nombre de risques, soit une cinquantaine par établissement.
- Développer une culture positive des contrôles entre autres en montrant leur nécessité. En parallèle il s'agit de faire la preuve que les contrôles ne sont pas synonymes de persécution tout en s'attachant à leur formulation.
- Idéalement avoir moins de contrôles que de risques. Cela pourrait aussi s'exprimer par avoir un minimum de contrôles pour couvrir le maximum de risques.
- Relever constamment le défi de la maintenance de tout ce qui a été mis en place.
- Et enfin ne jamais oublier notre vocation première qui est l'accueil et les soins aux personnes très âgées.

4 Les compétences et les ressources humaines nécessaires au fonctionnement du dispositif

1. REMARQUE LIMINAIRE

Mettre en place et surtout maintenir – le plus difficile – le dispositif de Contrôle Interne (DCI) (ou système de
Contrôle Interne (SCI)) ne peut s'envisager sans un minimum de ressources, et en premier lieu de nature humaine.
Ce besoin peut s'exprimer sous l'angle des compétences et des effectifs à mettre en ligne.
Trop souvent ce sujet est négligé et la volonté de mettre en place le contrôle interne peut se résumer en un simple acte de foi, sans concrétisation. Les motifs peuvent être objectifs (restrictions budgétaires par exemple) mais également résulter d'une mauvaise appréciation des conditions de réussite d'une mise en place d'un DCI. C'est donc une cause d'échec ou peut-être encore pire d'insatisfaction et de frustration. Le Contrôle Interne (CI) a un coût mais aussi en parallèle un retour sur investissement, hormis le côté de plus en plus obligatoire de la démarche.

2. QUEL DCI ET QUELLE GESTION DES RISQUES ?

C'est la première question qui doit être posée :
- Le périmètre du DCI se limite-t-il au comptable et financier ?
- La priorité est-elle donnée à la gestion (stratégique) des risques ?
- A l'inverse ne parle-t-on que de DCI sans les risques même si cela peut poser des problèmes ?

Des choix peuvent avoir déjà été faits au sein de l'organisme en matière d'organisation et de fonctionnement au regard des 4 niveaux définis par l'IFACI (souvent ramené à 3 par simplification) ?
Dans ce cadre la discussion entre SCI comptable et financier d'un côté, SCI opérationnel d'un autre côté, devient de plus en plus artificielle.
Même avec une approche au départ étroite, placée sous l'angle Sarbanes Oxley, le DCI peut en réalité couvrir en partie les aspects financiers et opérationnels si on considère que les événements redoutés engendrent dans la majorité des cas par des incidences financières (les processus liés au paiement de prestations sociales en sont un bon exemple). D'autre part avec COSO 3 se développe une approche complète (SCI financier + SCI opérationnel).

3. LES FACTEURS QUI PEUVENT IMPACTER LES BESOINS DANS UNE VISION LARGE DU SCI

Il s'agit d'éléments quantitatifs basés sur :
- Le nombre de processus et procédures,
- La nature des risques opérationnels et stratégiques,
- Le volume et la nature des prestations fournies et en particulier de nature financière,
- Le nombre de services internes, de départements, de directions composant la structure d'une entité,
- Le nombre de structures externes liées,
- Le volume et l'importance des modifications annuelles (législatives, organisationnelles, etc.) de diverses natures avec un impact sur une maintenance lourde,
- La nature des bases/exigences légales et réglementaires,
- Les remarques importantes contenues dans des rapports d'audits internes ou externes (voire d'une Cour des comptes),
- Le niveau de potentialités de fraudes interne et/ou externe,
- Les domaines de gestion analysés lors de l'audit des comptes,
- Le nombre et la nature des contrôles automatiques couverts par le système d'information.

Dans le domaine qualitatif, il peut être cité :
- la qualité et l'expérience des collaborateurs en charge du CI ;
- le niveau d'implication et/ou d'intérêt du management opérationnel ;
- l'utilisation d'un logiciel spécialisé en Contrôle Interne & risques ;

- le recours à un logiciel de modélisation (dans la mesure du possible en lien avec l'application CI) ;
- l'existence d'une application métier complète et structurante (y compris sur les aspects CI) ;
- la nature et/ou la complexité des activités ;
- une collaboration avec un spécialiste externe ;
- le niveau souhaité de maturité du CI ;
- la présence d'une culture du CI ancienne (même si on ne parlait pas encore de CI) ;
- le niveau d'exigences légales en particulier en lien avec le SCI financier ;
- l'homogénéité des activités ;
- le profil des clients/usagers

Parmi d'autres points, il peut être mentionné :

- La collaboration et la répartition des tâches entre les divers organes en charge des contrôles. Pour mémoire il s'agit des 3 (voire 4) niveaux entre l'opérationnel, le fonctionnel (fonctions dites supports) et l'audit interne.
- La question du testing (ou évaluation ponctuelle à mener par l'entité CI et/ou même en direct par l'opérationnel) des contrôles afin de s'assurer du bon fonctionnement du DCI est également importante.
- Le rôle que l'on veut attribuer au CI par rapport à celui dévolu à l'audit interne. En effet si le CI joue un rôle préventif, il sera amené non seulement à faire des tests mais aussi à porter un jugement plus axé sur la qualité. Autrement dit, il s'agira de détecter à la source les problèmes afin que l'audit interne en relève le moins possible. Ce facteur joue aussi si les rapports de l'audit interne sont diffusés, même de manière limitée, à la différence des comptes rendus de l'unité de CI qui sont essentiellement dédiés au responsable de l'entité concernée.
- L'existence d'un système qualité avec à la clé une certification. En effet le système qualité tend à se rapprocher du CI, notamment en ce qui concerne la prise en compte du volet risques. En conséquence les ressources dédiées à la Qualité semblent venir progressivement se « mélanger » avec celles relevant du CI, du moins en partie.

4. QUELLES RESSOURCES HUMAINES DÉDIÉES AU CONTRÔLE INTERNE (CI) : UNE PREMIÈRE PISTE CHIFFRÉE POUR LANCER LE DÉBAT

Peut-on facilement identifier un besoin minimum en contrôleurs internes (BMCi) ?
Par BMCi il s'agit des personnes exclusivement dédiées au CI (des « spécialistes » ou « professionnels ») ou partiellement en sus d'une autre responsabilité principale. Cependant comment alors considérer le temps consacré par plusieurs personnes pour des tâches relevant de près ou de loin du CI dans leurs activités courantes au niveau opérationnel, ou dans le cadre de leur fonction support.

L'exercice est difficile car il n'y aurait pas d'étude en la matière dans le secteur public voire même privé, même sur un SCI limité au financier. Il en serait de même pour le domaine du contrôle de gestion qui aurait pu donner quelques indications.
Par ailleurs, un nombre très important de paramètres peuvent intervenir (missions, tailles, niveaux de maturité du CI, etc.) et les comparaisons entre entités sont souvent ardues.
Toutefois ces dernières pourraient, peut-être, se faire sur des organisations de même type comme des établissements s'occupant de personnes âgées ou sur des départements. A un niveau plus fin, des services avec des missions proches pourraient être analysés.
Autrement dit, est-ce s'écarter du bon sens de penser que, dans une entité indépendante de 400 personnes, on devrait au moins disposer de l'ordre de deux spécialistes du CI ? A la louche, le besoin en contrôleurs internes minimum pourrait donc être - sur le principe et comme socle - de l'ordre de 0,5 à 1 % de l'effectif en phase de maintenance du DCI. A relever que le taux pourrait être sous-estimé sur un effectif bas et surestimé sur le haut.

5. LA RÉPARTITION DES BESOINS

Mais comment opérer dans la pratique la répartition de la dotation entre :

a) Ce qui peut être appelé le « central » en matière de Contrôle Interne soit sous la forme de services fonctionnels (niveau 2 des contrôles au sens de l'IFACI),
b) le niveau même d'une unité/service de Contrôle Interne (niveau 3),
c) Et l'opérationnel (niveau 1) ?

(Rappel : les niveaux 2 et 3 sont souvent regroupés en particulier dans le présent Livre blanc et le précédent).

La réponse n'est pas simple et il y aurait presque autant de réponses que d'entités. On peut cependant penser que jusqu'à une centaine de personnes (une institution pour personnes âgées par exemple), le taux global dédié au CI est plutôt entièrement regroupé en « central » tout en agissant aussi au niveau opérationnel. En revanche, lorsqu'on tombe dans des structures de plusieurs centaines de personnes avec des services opérationnels distincts, une répartition se fait de manière plus naturelle auprès des niveaux opérationnels.

De plus, une équipe centralisée de CI peut venir en appui, partiellement ou quasi totalement, à une petite entité CI dite opérationnelle. Cette tâche viendra en plus de celles d'animation, de coordination, d'expertise, de testing voire d'audit de premier niveau (ou « audit-terrain » ou évaluations ponctuelles de manière plus large).

Lors de la mise en place, les ressources à consacrer peuvent être largement supérieures (jusqu'à trois fois) sur un laps de temps court ; un appui externe étant même souvent requis.

Il est fondamental de rappeler dans ce contexte que toute organisation dispose d'éléments constituant un dispositif de Contrôle Interne, mais c'est souvent la formalisation et la réunion des pièces du puzzle qui fait défaut. De déclarer qu'avant il n'y avait rien et que maintenant il y a tout, comme on l'entend parfois, est le meilleur moyen pour démotiver tous les acteurs – actuels - du CI !

Le temps consacré à la maintenance du DCI peut prendre différentes formes : modifier un processus, adapter une directive, mettre à jour les risques, s'assurer de la qualité d'un contrôle, corriger un organigramme, organiser une campagne de contrôle, former les collaborateurs. A noter qu'une partie de ses tâches doivent de toute façon être réalisées avec, ou non, un Contrôle Interne clairement dénommé. Par ailleurs il y a le rôle CI qu'exercent les services fonctionnels sur l'organisme pris dans sa totalité en sus de la maintenance de leur propre dispositif de CI.

Dans ces chiffres, le temps consacré, par exemple par les opérationnels, à des contrôles ou à des autocontrôles n'est pas pris en compte. Il en va de même lorsqu'un manager réfléchit à ses risques. Ces tâches font parties intégrantes de leurs activités.

Le temps dédié peut émaner d'une ou de plusieurs personnes avec des casquettes diverses. Il peut s'agir de contrôleurs internes, de répondants CI (soit réalisant à côté d'autres tâches des activités de CI de manière décentralisée), de correspondants CI (soit un simple relai entre un service central de CI et une entité opérationnelle), de contrôleurs de gestion, de contrôleur budgétaire, …

Par contre dans une plus petite organisation (de 100 à 200 personnes) les tâches de CI peuvent être réparties sur plusieurs personnes plus généralistes. Dans les plus grandes il y aurait concentration du CI sur des « spécialistes » localisés au niveau de l'opérationnel et/ou d'une fonction support.

Tous les cas de figure sont donc possibles d'où la grande difficulté de fixer une règle uniforme.

6. LES BESOINS QUALITATIFS (OU QUALITÉS DES PERSONNES DÉDIÉES AU CI)

Posé sous un autre angle, est-ce que le spécialiste en Contrôle Interne a des caractéristiques propres qui le différencient par exemple d'un contrôleur de gestion ? Que vaut-il mieux : un comptable qui étend son champ d'expertise au CI (via de la formation) ou un contrôleur interne avec de bonnes connaissances comptables ?

Les compétences nécessaires sont-elles différentes pour respectivement le SCI financier et le SCI dans une vision élargie ?

Au niveau central faut-il d'autres qualités qu'au niveau opérationnel pour exercer ce métier ? Quelle est la bonne filière pour devenir un bon spécialiste du Contrôle Interne ? Les personnes issues de l'audit interne (voire externe) font-elles des contrôleurs internes performants ? A l'inverse peut-on passer du CI à l'audit interne ?

Si on considère le système de Contrôle Interne (SCI) comme un système de management intégré, s'appuyant sur deux composantes essentielles que sont la gestion des risques et le Contrôle Interne, définies au sens du référentiel COSO *(cf. Livre blanc No 1 page 87)*, est-ce que les besoins qualitatifs sont identiques versus différents pour chacune de ces deux « branches » ?

Faut-il mieux quelqu'un issu du métier qui se forme au CI ou une personne qui se forme au CI puis travaille sur/avec le métier ? Un spécialiste qualité fera-t-il un contrôleur interne de qualité ?

Les qualités requises d'un professionnel du CI sont-elles différentes ou identiques entre le secteur public et privé ?

Comment doit-on considérer des éléments comme :

- sens de l'éthique
- curiosité
- généraliste
- connaissances comptables
- persévérance
- rigueur
- motivateur
- communicateur
- esprit analytique.

Une large enquête sur la question serait des plus intéressantes afin de donner quelques pistes au recruteur d'un contrôleur interne ou à la hiérarchie opérationnelle pour « dénicher » dans ses collaborateurs la personne la plus adéquate.

7. CONCLUSIONS

Elles sont au nombre de cinq.

Premièrement une démarche de CI ne peut se faire qu'avec des ressources qualitativement et quantitativement adaptées tant en phase de mise en place que de maintenance. Ces ressources prennent des formes différentes : professionnel du CI, activité de CI en sus d'une autre responsabilité, ou être identifiées et définies dans la fiche de poste d'un contrôleur de gestion ou de responsable qualité, par le manager métier, par la personne allouée à l'exécution d'une tâche opérationnelle, etc.

Deuxièmement les compétences et qualités des contrôleurs internes pourraient être moins complexes à cerner.

Troisièmement il y a en l'état une grande difficulté à fixer la bonne dotation au niveau de chaque acteur : du service opérationnel en passant par les services fonctionnels et pour arriver à une éventuelle entité CI central. Ce constat découle déjà de situations très différentes mais ce qui n'exclurait pas un benchmark sur des situations assez comparables. Cet exercice serait-il plus simple si on se limitait au SCI strictement financier ?

Cependant et cela sera le quatrième point, quelques ordres de grandeur peuvent être définies à titre d'hypothèse afin de lancer une approche de DCI en termes de BMCi, Ainsi est-il (dé)raisonnable de considérer qu'un BMCi de 0,5 à 1,0% appliqué respectivement sur la taille (nombre total de personnes) :

- de l'entité considérée (le service par exemple)
- puis sur le total de l'organisation (un établissement public, un département, etc.).

Pour résumer un taux de 1 à 2% sur la taille donne-t-il une idée de l'enveloppe nécessaire en CI ? Cette dernière devant alors être ventilée.

Dans une entité de 100 à 200 personnes – cas de figure peut-être plus simple - d'une certaine complexité(processus nombreux, poids des règles légales, rythme des changements, etc.) est-ce qu'au moins un contrôleur interne professionnel ferait sens ?

La fourchette annoncée est relativement large mais elle est à la hauteur de la diversité des contextes… et des incertitudes ; par ailleurs le BMCi pourrait évoluer (à la baisse ? à la hausse ?) au fil du temps. Néanmoins le pourcentage est moins défendable avec l'augmentation de la taille car le nombre de personnes exerçant le même métier s'accroit mais sans justifier une croissance linéaire de la dotation. Il faut ainsi reconnaître l'impossibilité à ce stade de fixer à partir de où un effet de seuil apparaît sur l'effectif à considérer.

Enfin, comme **cinquième et dernière conclusion**, le but final poursuivi est de lancer la réflexion, et en amont une prise de conscience, sur ce thème capital des ressources humaines nécessaires en qualité et en quantité. Si les réponses formulées dans ce rapport peuvent entraîner de légitimes interrogations, en particulier sur l'aspect quantitatif et ainsi créer une certaine insatisfaction, il n'en demeure pas moins que ces quelques analyses sauront renforcer lebon sens des animateurs du Contrôle Interne - et de leurs responsables - dans la détermination des ressources humaines nécessaires au fonctionnement du dispositif.

5

Le role des systèmes d'informations dans le dispositif de Contrôle Interne

Les conséquences d'un mauvais fonctionnement du SI sur les risques d'une entité sont évidentes et de plus en plus nombreuses, tant le rôle joué par les SI dans le comportement d'une organisation est devenu important.
Le SI est à la fois créateur de risques et également instrument de contrôle interne pour parer à ces risques.
Le tableau qui est présenté ci-après et les développements qui s'ensuivent ont pour objet de présenter les différentes situations où le SI et son administration impactent de manière significative la maîtrise des risques d'une organisation.

1. LES CAUSES DE SURVENANCE D'UN RISQUE

Les causes de survenance du risque SI

A. LIEES A LA GOUVERNANCE DES SI

Causes	Impact	Exemples
Mauvaise clarification du niveau de pouvoir de décision (Tutelle, chef d'établissement, DSI locale vs DSI de Tutelle)	Qualité sur les SI	
Méconnaissance des enjeux et de la montée de la mise en place d'un SI efficace et efficient pouvant contribuer à l'atteinte des objectifs stratégiques		
Mauvaise relation entre le DSI et le décideur et entre le DSI et les métiers	Ne répond pas aux attentes de la direction et au besoin métier.	
Mauvaise organisation du service informatique / mauvais pilotage de la part du DSI	Retard dans la mise en place des projets de transformation/ Mauvaise anticipation des besoins	

A. LIEES AU COMPORTEMENT UTILISATEUR ET A L'ORGANISATION DES SERVICES

Causes	Impact	Exemples
Plan de formation des utilisateurs (interne) / manque d'information ou ergonomie mis en mal conçue (interne) / sous-dimensionné/inadapté. Absence de contrôle lors de la saisie	Mauvaise compréhension des conséquences de leurs actions / Qualité de la données (exhaustivité, exactitude, conformité, etc.) Mécontentement de l'usager (moral? financier, juridique, image, etc.)	Utilisation d'un code Y au lieu d'un code Y, alors que les codes sont ensuite utilisé pour identifier le type de population bénéficiaire du dispositif
Documentation de l'application inexistante/incomplète/non mise à jour/indisponible	Biais de calcul + Perte de fiabilité de la donnée / Reporting erroné	
Malveillance avec l'intention de nuire / Environnement		
Absence de manuel d'organisation		
Perte de connaissance et de compétences de la part de la DSI (suite à départ par exemple)		

B. LIEES A L'INADAPTATION DU PROGRAMME INFORMATIQUE AUX BESOINS FONCTIONNELS ET REGLEMENTAIRES

Causes	Impact	Exemples
Paramétrages/règle de calcul non conformes au besoin Mauvaise réalisation technique Tests et recette insuffisants Absence de comité de cohérence entre les besoins des utilisateurs et les fonctionnalités proposées dans le outils Langage informatique obsolète (ERP) ne décrit clairement le besoin fonctionnel	Données de sortie non fiables / insatisfaction des bénéficiaires	Biais dans le calcul des primes dûes en fonction des dates d'entrée et de sortie
Mauvaise compréhension ou interprétation du règlement /Traduction du besoin métier non conforme aux règles comptables et juridiques Mauvaise traction du règlement d'un point de vu fonctionnel (GDC)	Non certification de la part des Commissaires aux Comptes	Impossibilité technique d'associer ou rattachement des charges de masse salariale à l'exercice
Contrôles embarqués dans les applications insuffisants/non mis à jour		Paiement d'heures complémentaires alors que l'agent dépasse le plafond autorisé
Manque de communication entre fonctionnel et DSI /	Rejet par l'utilisateur	
	Ne permet pas de répondre aux besoins nouveaux des utilisateurs	
Connaissance et maintenance du parc informatique insuffisante	Panne / indisponibilité / lenteur du matériel	Transmission des éléments à harmoniser à la Trésorerie générale non, délai + non paiement des agents pour le mois en cours
Absence de la prise en compte des recommandations/besoins du comité interne	Absence de contrôle automatique	

C. LIEES AUX ASPECTS TECHNIQUE ET DE SECURITE

Causes	Impact	Exemples
Mauvaise gestion des droits d'accès au système d'information	Confidentialité des données non sécurisé	Un personnel non autorisé accède aux données de paie - Risque de divulgation d'informations confidentielles
	Risque de fraude	- Risque de s'octroyer des rémunérations
	Risque de détérioration de la donnée (perte de qualité et d'intégrité)	
Perte de connaissance et de compétences de la part de la DSI (suite à départ par exemple)		
Plan de protection du matériel physique insuffisant		
Mauvais dimensionnement du dispositif de sauvegarde et de continuité	Restauration des données impossible + perte d'informations	
Absence de RSI		
Absence de PCI.		
Absence de test de montée en charge		

D. LIEES A LA QUALITE D'INFORMATION (Exhaustivité, intégrité, piste d'audit, traçabilité...)

Causes	Impact	Exemples
Architecture du SI inadaptée à l'organisation	Coût du SI non maîtrisé	Multiplication des outils pour traiter le processus paie (de la gestion du dossier à l'intégration des données en comptabilité) dans le intégré + multiplication des coûts de maintenance, de développement, des coûts de personnels
Absence de schéma directeur du SI (ou de suivi du schéma directeur)	Redondance des données multiples / perte de temps et de fiabilité	
Absence de contrôles (intégrité, exhaustivité, etc.)	Développement de bases de données parallèles propres à chaque service + pas de partage de l'information + difficulté de reporting	
Rupture de la piste d'audit	Risque de faire des choix politiques sur la base de données erronées	
Application obsolète	Couverture des besoins limitée + manque d'indicateurs pour la prise de décision	
	Absence d'outil de pilotage décisionnel /	
	Disponibilité / intégrité /exhaustivité / traçabilité des données non assurée.	Impossibilité de mesurer le respect du plafond de masse salariale et du plafond d'emploi
Application nouvelle avec bugs / instable		
Délai de mise à disposition des données pour traitement/analyse trop long	Disponibilité tardive des données pour la prise de décision + délai trop long pour la mise en œuvre d'un plan d'action	
Perte de données lors de l'interfaçage entre les différentes applications pour le transfert des données / Mauvaise intégration des flux	Fiabilité non assurée / Risque d'altération des données	Une paye effectuée par trésorerie générale mais non intégrée dans la comptabilité de l'établissement, une prime intégrée dans un compte comptable de "charge patronale"

2. RISQUES LIÉS À L'ADMINISTRATION DU SI (SYSTÈME D'INFORMATION)

Les conséquences d'un mauvais fonctionnement du SI sur les risques d'une entité sont évidentes et de plus en plus nombreuses, tant le rôle joué par les SI dans le comportement d'une organisation est devenu important.

Le SI est à la fois créateur de risques et également instrument de contrôle interne pour parer à ces risques.

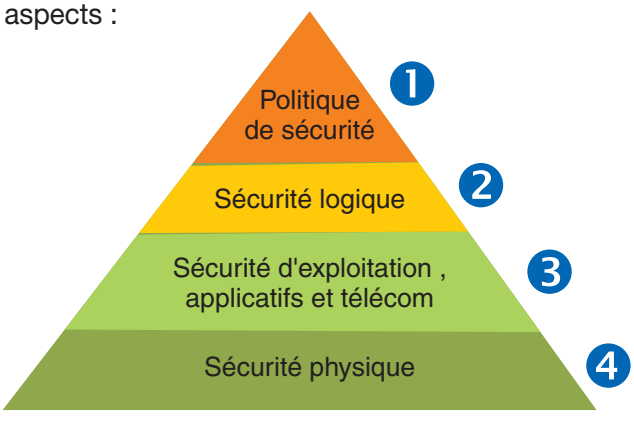
Le tableau qui est présenté ci-après et les développements qui s'ensuivent ont pour objet de présenter l

2.1 Introduction

Avec le développement de l'utilisation d'Internet, de plus en plus d'administrations publiques ouvrent leur système d'information à leurs partenaires, à leurs fournisseurs ou externalisent en mode SAAS (Software as a Service). Il est donc essentiel de connaître les ressources de l'administration publique à protéger et de maîtriser le contrôle d'accès et la gestion des habilitations du système d'information.

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles permettant de les stocker ou de les faire circuler. Il représente une partie du patrimoine de l'administration publique ; il fait partie des immobilisations comptables.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Il convient donc d'aborder d'une manière **globale la sécurité** en prenant en compte tous ses aspects :



Domaines de la sécurité informatique

❶ *La politique de sécurité incluant la sensibilisation des utilisateurs aux problèmes de sécurité.*

❷ *La sécurité logique, c'est-à-dire la sécurité au niveau des données, les applications ou encore les systèmes d'exploitation.*

❸ *La sécurité d'exploitation, applicative et des télécommunications.*

❹ *La sécurité physique, soit la sécurité au niveau des infrastructures matérielles.*

On distingue deux types d' « insécurité » :

- L'état actif d'insécurité, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système d'information, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur).

- L'état passif d'insécurité, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

La sécurité informatique vise cinq principaux objectifs :

- L'intégrité, qui permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.

- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;

- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ;

- La non répudiation, permettant de garantir qu'une transaction ne peut être niée ; les notions d'imputabilité, de traçabilité et d'auditabilité sont associées à la non répudiation (impossibilité de refuser un événement qui a eu lieu).

- L'authentification, consistant à assurer que seules les personnes autorisées ont accès aux ressources.

Si les cinq principaux objectifs ne sont pas couverts, **la liste des risques augmente considérablement (liste non exhaustive) :**

- **Le risque de fraude** par le détournement du système de paie, par exemple ;

- **Le risque de vol** ;
- **Le risque de non-conformité juridique** par le non-respect des lois (la CNIL[10] et la LOLF) ;
- **Le risque opérationnel** par l'augmentation de délai d'administration des systèmes (perte en efficacité et réactivité des services opérationnels) ;
- **Le risque de régression** dans le cas de développement de nouvelles évolutions ;
- **Le risque de confidentialité** par la divulgation de données sensibles (dossier du patient à l'hôpital, par exemple).

PRÉSENTATION DES RISQUES	PARADES PROPOSÉES
Risque de fraude	- Le rappel aux agents des règles de sécurité générale sur l'utilisation du matériel informatique ; - L'information des agents des différentes attaques ou vols ayant un lieu dans l'administration ; - La mise en oeuvre d'une charte d'utilisation des systèmes d'information rappelant le bon usage de la téléphonie, de la messagerie électronique, du portail, d'Internet, téléphone portable.
Risque de vol	- Les locaux doivent faire l'objet d'une sécurisation particulière : vérification des identités à l'accueil, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs. - La mise en place de badge pour accéder au service comptable ; - La mise en place d'une gestion d'habilitation permettant la restriction de l'accès aux transactions les plus sensibles et l'attribution d'un compte à une personne physique avec un statut (actif ou suspendu) par rapport à sa fonction ;
Risque de non-conformité juridique	- La sensibilisation continue des collaborateurs aux enjeux et principes découlant de la règlementation CNIL ; - La mise en place de veille réglementaire ; - Une évolution permanente des politiques de sécurité, de gestion des droits, etc.
Risque opérationnel	- La mise en place d'outils techniques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc et un contrôle par monitoring des interfaces entre les applications fonctionnelles et métiers; - La mise en place de chartre de qualité de service entre le client (agents) et le fournisseur (direction informatique) - La mise en place d'un plan de continuité[11] et de reprise, testés deux fois par an.
Risque de régression	- La mise en place d'une gestion de projet pour l'intégration de nouvelles applications; - La réalisation de tests fonctionnels et techniques sur les applications développées; - La prise en compte de la vulnérabilité des systèmes lors de mise en production de nouveaux développements
Risque de confidentialité	- Le cryptage des données sensibles ; - La mise en place d'un serveur dédié aux interfaces avec un mot de passe ; - La mise en place d'une clause de confidentialité pour chaque prestataire.

10 CNIL : Commission Nationale de l'Informatique et Libertés
11 Pour plus d'information sur la mise en place d'un Plan de Continuité d'Activité, merci de vous reporter à l'annexe 1 du présent ouvrage.

L'insécurité active ou passive, conjuguée aux différents risques ont un impact sur l'image, sur l'activité et sur les équilibres financiers des administrations.

2.2 La mise en place d'une politique de sécurité

La politique de sécurité reflète la vision stratégique de l'établissement publique en matière de sécurité des systèmes.

Sa rédaction requiert l'inventaire des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information incluant de nos jours des éléments comme les équipements mobiles (téléphone portable, tablettes,…) ou encore des objets connectés (bracelet de santé, par exemple) :

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'administration publique et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.
- Valider son contenu par la Direction Générale ;
- Communiquer à l'ensemble des utilisateurs.

Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'administration concernée.

Par exemple, l'absence de politique de sécurité pourrait entraîner des usages non appropriés du système d'information (exemple dans le cas d'une Université) :

- *Téléchargement d'application non toléré conduisant à un ralentissement des serveurs ;*
- *Copie à partir d'un disque externe USB conduisant à l'infiltration de virus;*
- *Utilisation de la messagerie professionnelle à des fins privées conduisant à un retard dans le traitement des factures fournisseurs.*

La parade est la mise en place d'une politique de sécurité :

- *Le rappel aux agents des règles de sécurité générale sur l'utilisation du matériel informatique ;*
- *L'information des agents des différentes attaques ou vols ayant un lieu dans l'administration ;*
- *La mise en oeuvre d'une charte d'utilisation des systèmes d'information rappelant le bon usage de la téléphonie, de la messagerie électronique, du portail, d'Internet, téléphone portable.*

La sécurité informatique de l'administration publique repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès d'eux ; mais elle doit aller au-delà et couvrir les champs de la sécurité logique.

2.3 La sécurité logique appropriée aux différents membres du personnel

La sécurité logique consiste à gérer le cycle de vie du personnel dans le système d'information selon leurs fonctions et leurs directions de rattachement. Elle repose sur la mise en oeuvre d'un système de contrôle d'accès s'appuyant sur un service d'authentification, d'identification et d'autorisation.

Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier le degré de sensibilité (du moins confidentiel au plus confidentiel) et limiter les risques :

- **Risque de non confidentialité** des données ;
- **Risque de fraude** dans le cas de non séparation des fonctions ;
- **Risque de malveillance** dans le cas d'une mauvaise gestion des mots de passe ;
- **Risque de conformité** par le non-respect des lois (CNIL, par exemple).

Risque de non confidentialité des données : Les données ne doivent être accessibles qu'aux personnes habilitées dans l'exécution des missions qui leurs sont confiées.

Il en est de même pour les prestataires externes. Leurs interventions doivent être encadrées par une clause de confidentialité à l'égard des données auxquels ils peuvent avoir accès.

Concernant les données qui sont gérées à l'extérieur de l'administration publique (Cloud, mode Saas), en amont de la signature du contrat, le directeur informatique et la direction juridique doivent vérifier que les données externalisées sont bien protégées et que leurs confidentialités sont assurées.

Enfin, le matériel informatique et mobile en fin de vie, tels que les ordinateurs, tablettes, portables, doivent être expurgés de leurs disques durs avant d'être donnés ou détruits.

Par exemple, l'absence de confidentialité au sein d'une administration peut conduire à :

- *La divulgation du fichier des primes des agents ;*
- *Les fichiers d'interface de paie accessibles sur le réseau ;*
- *L'utilisation frauduleuse du fichier abonné par un sous-traitant.*

La parade est :

- *Le cryptage des données sensibles ;*
- *La mise en place d'un serveur dédié aux interfaces avec un mot de passe ;*
- *La mise en place d'une clause de confidentialité pour chaque prestataire.*

Risque de fraude : La séparation des fonctions dans un environnement fortement informatisé est liée à la gestion des habilitations informatiques. Elle permet de renforcer le Contrôle Interne et de prévenir la fraude entre la personne qui réalise une tâche, la seconde qui la valide et la dernière qui la contrôle.

L'administration des comptes utilisateurs, la gestion de l'accès aux postes de travail et du système d'information garantissent un niveau de sécurité. L'administration consiste à la création de comptes utilisateurs nominatifs
attribués aux utilisateurs selon leurs fonctions. Il revient donc aux responsables hiérarchiques de définir les droits d'accès. Ces comptes nominatifs permettent de mémoriser l'origine du message et garantir la présence d'informations nécessaire à l'analyse ultérieure d'événements (transactions sur les comptes bancaires).

La procédure est aussi applicable aux administrateurs systèmes et réseaux et aux autres agents chargés de l'exploitation du système d'information.

Par exemple, le risque de fraude au sein d'une administration peut conduire à :

- *La saisie d'un agent de sa propre paie;*
- *Utilisation d'un « générique » ne permettant pas d'identifier précisément une personne qui réalise la tâche (modification du SIRET sur le référentiel fournisseur) ;*
- *La non clôture des comptes pour les stagiaires ou les CDD saisonniers ;*

La parade est :

- *La création d'une matrice de séparation des tâches entre les différents agents intervenants dans le processus ;*
- *La restriction de l'accès aux transactions les plus sensibles et l'attribution d'un compte à une personne physique avec un statut (actif ou suspendu) par rapport à sa fonction ;*
- *Le paramétrage de début et de fin des comptes nominatifs ouverts avec la mise en place régulier de contrôle.*

Risque de malveillance : La première protection contre la malveillance ou la fraude est la gestion des mots de passe. Le mot de passe permet l'accès à un poste de travail informatique et aux logiciels. Il doit être individuel, difficile à deviner et rester secret.

Ces mots de passe, ainsi que des dispositifs antivirus, doivent être installés également sur les appareils mobiles ou les tablettes ; ces équipements doivent être suffisamment protégés car connectés à la fois au système d'information et à l'extérieur.

La connectivité GPS permet la localisation de l'équipement en cas de perte ou de vol, sous réserve du respect de la règlementation en vigueur.

Par exemple, l'absence de politique de mot de passe au sein d'une administration peut conduire :

- *L'introduction d'un virus dans le serveur applicatif comptable;*
- *Un tiers utilise le téléphone portable d'un agent ;*
- *Un agent se connecte à partir d'un ordinateur d'un collègue.*

La parade est :

- *Le déploiement sur tout le matériel informatique d'antivirus avec une mise à jour régulière ;*
- *Le verrouillage du matériel mobile avec une modification de mot de passe régulière ;*
- *Un contrôle automatique à l'aide du système qui contraint l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment. Il doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois).*

Risque de non-conformité juridique : La loi "informatique et libertés" du 6 février 1978 réglemente l'utilisation des
fichiers contenant des données nominatives. Elle définit les obligations de protection et de déclaration des données personnelles et de leurs traitements à la CNIL.

Par exemple, le non-respect de la loi « informatique et libertés » peut conduire à :

- *La divulgation des données de ressources humaines;*
- *L'accès aux données médicales du patients ou résident peut faire courir des risques sur la vie privée des personnes concernées ;*
- *L'utilisation des photos à des fins commerciales sans demander au préalable une autorisation.*

La parade est :

- *La sensibilisation continue des collaborateurs aux enjeux et principes découlant de la règlementation CNIL ;*
- *La mise en place de procédure claire sur l'éthique et le secret professionnel et son explication aux agents ;*
- *Une évolution permanente des politiques de sécurité, de gestion des droits, etc.*

La sécurité logique doit être complétée par une sécurité renforcée des réseaux et applicatifs et une administration.

2.4 La sécurité d'exploitation, applicative et télécom renforcée par des nouveaux outils

La sécurité d'exploitation concerne tout ce qui touche au bon fonctionnement du système. Ceci comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de test, de diagnostic, de mise à jour, de sauvegarde et d'archivage. La sécurité de l'exploitation dépend fortement de son degré d'industrialisation et de son niveau de supervision.

La sécurité des télécommunications doit permettre d'offrir aux agents une connectivité fiable et de qualité de « bout en bout ». Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communications, des systèmes d'exploitation et des équipements mobiles et connectés.

Il est donc déterminant de mettre en place des protections applicatives et réseaux pour tendre vers un risque minimal, réduisant ainsi les impacts d'image et financiers qui pourraient en découler.

Les principaux risques identifiés sont :

- Risque de régression des applications ;
- Risque de continuité d'exploitation.

Risque de régression : La mise en production de nouveaux logiciels ou des évolutions applicatives ou logicielles nécessitent le respect de la méthodologie de gestion de projet informatique qui se décline en plusieurs phases :

- la conception en intégrant la robustesse des applications ;
- les développements des contrôles programmés ;
- la réalisation de jeux de tests,
- l'élaboration d'un plan de migration des données,
- la validation conjointe de la MOE/MOA du programme avant sa mise en production,
- la mise en production après avoir prévu un plan de retour dans le cas d'une anomalie ou régression applicative.

Par exemple, le non-respect de la gestion de projet peut conduire à :

- *Un développement logiciel ne correspondant pas aux besoins utilisateurs ;*
- *Un nouveau développement qui écrase un seuil de validation achat lors d'une validation de commande fournisseurs;*
- *Un arrêt logiciel de réservation voyageur.*

La parade est :

- *La mise en place d'une gestion de projet ;*
- *La réalisation de tests fonctionnels et techniques ;*
- *La prise en compte de la vulnérabilité des systèmes lors de mise en production de nouveaux développements.*

Risque de continuité d'exploitation : La continuité d'exploitation est assurée par la mise en place d'un canal de communication fiable entre les correspondants à l'aide d'un réseau sécurisé au niveau des accès, protocole, systèmes d'exploitation et d'équipements. Il doit déjouer des attaques (intrusion, recherche de mot passe, exploitation de la faiblesse du réseau TCP/IP, téléchargement des données du Cloud,…), des connections à distance ou des accès Internet.

La continuité de service est aussi garantie par la politique de sauvegarde et d'archivage de données.

L'opération de sauvegarde consiste à dupliquer

puis à mettre en sécurité les données contenues dans le système d'information.

- Les sauvegardes régulières permettent le stockage des données sur des espaces serveurs ou sur des supports externes. Ils doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé.
- Les serveurs hébergeant des données sensibles doivent être absolument sauvegardés et redondés. En parallèle, il est recommandé d'écrire une procédure « urgence – secours » qui expliquera comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur.

Les données peuvent faire l'objet d'archivage ; il consiste à enregistrer des données pour permettre la conformité à l'administration fiscale. Il est recommandé de les archiver à l'extérieur de l'administration, chez un prestataire spécialisé.

Par exemple, l'absence de sécurisation du réseau peut conduire à :

- *Une attaque des serveurs ne permettant plus aux étudiants le paiement en ligne des inscriptions ;*
- *L'interception de message confidentiel lors de connexion à distance ;*
- *La perte de données de facturation lors d'arrêt serveur.*

La parade est :

- *La mise en place d'outils techniques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc et un contrôle par monitoring;*
- *La mise en place de connexion distante sécurisée, par l'intermédiaire de liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel) ;*
- *La mise en place d'un plan de continuité et de reprise, testés deux fois par an.*

Le dernier niveau de sécurité informatique est la sécurité physique.

2.5 La sécurité physique au service de l'informatique

La sécurité physique concerne tous les aspects liés à l'environnement dans lequel les systèmes d'information se trouvent. Elle protège l'ensemble des biens du système d'information par le déploiement des normes de sécurité, des protections de l'environnement, l'élaboration de plan de maintenance préventive,….pour éviter notamment le risque sur la continuité d'exploitation.

Risque de continuité d'exploitation : L'activité est assurée si l'environnement du système d'information est protégé.

Le contrôle d'accès physique est un dispositif permettant un accès contrôlé à un lieu, à un bâtiment, à un local, à une machine ou à des équipements spécifiques.

Par exemple, la faiblesse de la sécurité physique peut s'illustrer par :

- *Un visiteur qui accède à la salle serveur ;*
- *Un serveur d'application de paie s'arrête faute de pièce ;*
- *Un incendie qui se déclare dans la salle serveur en absence de climatisation.*

La parade est :

- *Les locaux doivent faire l'objet d'une sécurisation particulière : vérification des identités à l'accueil, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs.*
- *La mise en place de mesures préventives et correctives (pièce de rechange, contrat de maintenance…)*
- *La protection du matériel par l'installation d'onduleur, d'extincteur, de climatisation dans la salle machine.*

Le progrès des technologies de l'information et l'ouverture des systèmes sur l'Internet contraignent les administrations à se protéger des risques (attaques, fraudes, vol, erreurs humaines) par la mise en place de la sécurité du système d'information sur l'ensemble des domaines (politique, logique matériel et physique).

3. LES RISQUES LIÉS À LA GOUVERNANCE DES SI

3.1 Introduction

La gouvernance des systèmes d'information va de pair avec la gouvernance d'entreprise ou d'administration[12].
Elle assure que son activité est cohérente avec la stratégie de l'organisation (entreprise, administration,…) tout en garantissant à la

Direction Générale et au Conseil d'Administration que la fonction informatique est convenablement pilotée.

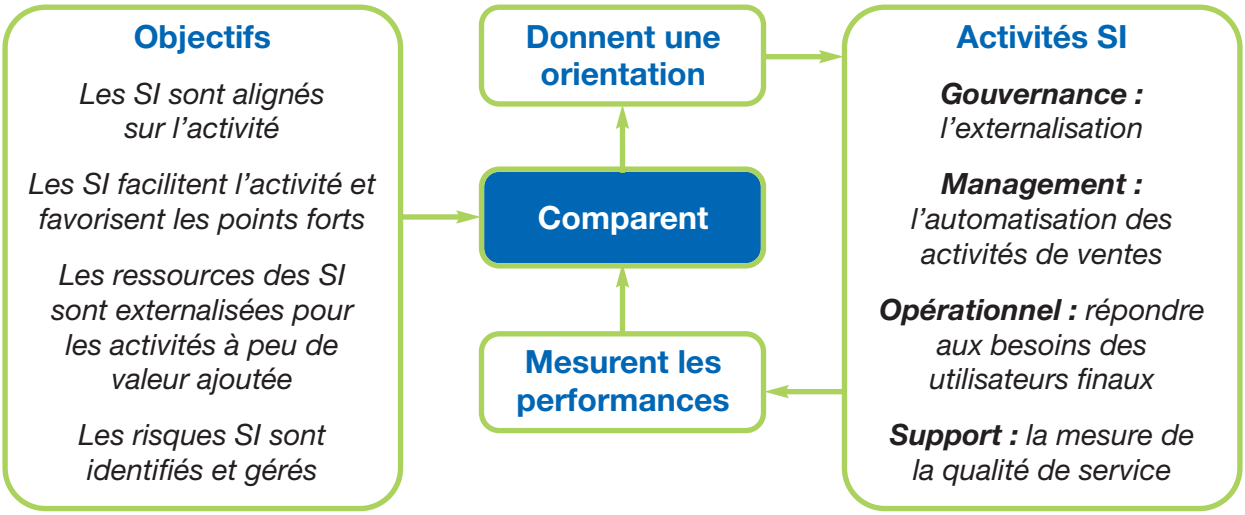
On rappelle ici que la gouvernance d'entreprise s'adresse principalement aux instances externes (Conseil d'Administration, Tutelle,….). Elle est pilotée par le Conseil d'Administration, puis la Direction Générale exécute au quotidien les opérations afin :

- De veiller à ce que l'ensemble des orientations et des pouvoirs délégués soit bien compris ;
- D'identifier les processus et les activités qui font partie intégrante de la mise en oeuvre des orientations fixées par le Conseil d'Administration ;
- D'évaluer des facteurs (de risques) pour lesquels les objectifs ne pourraient être atteints.

Aujourd'hui, les grandes organisations ont mis en place, selon leurs niveaux de maturité des instances, des référentiels (COBIT, Risk IT) ou des entités pour maîtriser les vastes programmes de transformations liées aux systèmes d'information. Ces programmes, définis au travers de 5 piliers (ITGI[13]), ont pour objectifs :

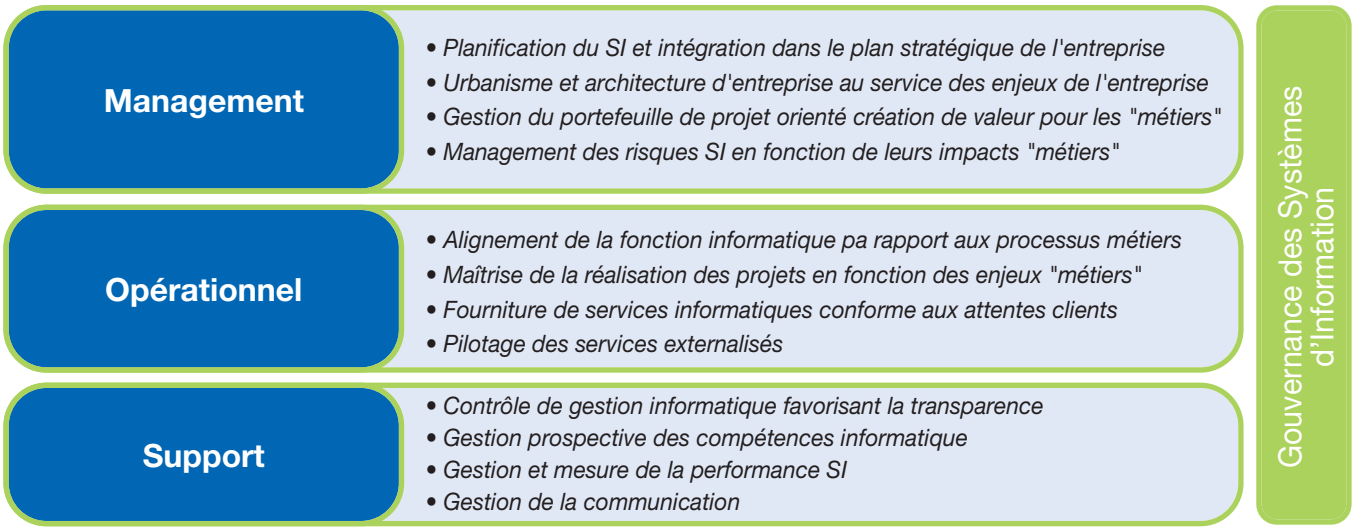
- D'aligner les systèmes d'information avec les objectifs de l'entreprise ou de l'administration ;
- De créer de la valeur au travers des systèmes d'information ;
- De gérer les risques informatiques ;
- D'améliorer la performance de l'organisation ;
- De gérer les ressources informatiques.

Cadre de gouvernance des SI[14]



Le cadre de gouvernance des systèmes d'information couvre tous les métiers des systèmes d'information.

Les activités de gouvernance des SI[15]



12 Cf. LOLF
13 Institut de gouvernance de la technologie de l'information
14 Board Briefing on IT Governance, 2 Edition, 2003
15 Audit et Contrôle Interne, IFACI N°206, septembre 2011

La gouvernance doit permettre la création de valeur, la gestion des risques, la maîtrise des coûts et garantir la qualité de service, assurant :

- La transparence de l'information ;
- L'accessibilité à l'information ;
- La fiabilité des données ;
- La sécurité des données ;
- La traçabilité de l'information.

La gouvernance des systèmes d'information

La gouvernance doit être intégrée aux métiers de l'entreprise ou de l'administration. La gouvernance des SI est fortement liée à l'implication de la Direction Générale. Cette dernière doit appuyer sa direction informatique dans les programmes de transformation (perçus souvent comme trop longs, trop coûteux,…).

Pour la réussite d'un projet, il est nécessaire de clarifier sa position par rapport à la stratégie d'entreprise ou de l'administration, d'identifier les besoins et de revisiter les responsabilités de chacun.

Il en est ainsi de l'informatique qui est au service de la stratégie et doit être organisée en fonction des objectifs qui lui ont été définis et non développer des projets de manière opaque sans tenir compte des opérationnels et des évolutions technologiques.

La création d'une centrale d'achat entre plusieurs administrations, par exemple, est une décision relevant de la Direction Générale, dont les membres doivent avoir une compréhension des enjeux pour gérer, d'une manière collégiale, les priorités et les solutions.

Ce schéma de fonctionnement permet de responsabiliser chacun dans sa fonction et d'éviter la dilution des responsabilités et le maintien d'un « fonctionnement historique » et en silos.

La gouvernance informatique s'appuie, selon leur niveau de maturité, sur des instances de décision ou d'arbitrage. Elles doivent valider la faisabilité technique, financière (ROI) et stratégique (besoin et enjeux) de projets tout en évaluant les risques. Une gouvernance faible peut conduire à une absence de priorisation des projets et des prises de décisions mal définies qui se caractérisent, par exemple, par un pilotage uniquement par les coûts ou par le lancement d'un projet de centralisation très complexes ; par exemple la création d'un logiciel unique pour l'ensemble d'un Ministère. Des bonnes pratiques pour limiter les risques :

- S'assurer que les SI font partie du processus de planification stratégique ;
- Aligner la stratégie en matière de SI avec les objectifs organisationnels ;
- Confirmer l'existence d'un comité directeur des SI.

Cette gouvernance des SI ne peut pas être totalement efficace sans un dispositif de collaboration efficace entre les directions opérationnelles et la DSI.

3.2 La création de valeur adaptée

L'investissement engagé pour des projets des SI apporte de la valeur ajoutée à l'entreprise ou à l'administration si ceux-ci sont réalisés sur des projets innovants. Le développement des nouvelles technologies et l'industrialisation de certains métiers conduisent à des gains de productivité (par exemple, l'achat en ligne de billet de train et sa dématérialisation).

Les investissements sont choisis à partir du portefeuille de projets co-construits avec les directions opérationnelles.

Puis, le projet doit être suivi durant tout son cycle de vie conjointement par les opérationnels métiers et par les équipes informatiques.

Naturellement, la fonction informatique doit être en mesure de démontrer sa véritable contribution à l'entreprise ou à l'administration, c'est à dire elle doit à la fois gérer des infrastructures existantes et développer de nouvelles applications tout en respectant les coûts, les délais et les objectifs de qualité de service. Ces choix doivent être motivés et compte tenu des risques, se permettent d'utiliser des logiciels « open sources » non maintenus.

Des bonnes pratiques pour limiter les risques :

- Définir les éléments déclencheurs et les objectifs de la prestation de services avec une réflexion préalable de 6 mois ;
- Identifier efficacement les besoins ;

- Définir des plans de communication pour les nouveaux projets;
- Suivre les projets sur les délais et les coûts et la réponse aux besoins utilisateurs;
- Atteindre les objectifs fixés;
- Réaliser les ROI d'un projet pas uniquement sur le critère financier mais également sur la valeur ajoutée apportée à l'entreprise ou à l'administration.

3.3 Alignement stratégique et une gestion du risque

La gestion du risque a pour objectifs la protection des systèmes d'information, la reprise ou la continuité des activités. Elle permet également d'arrêter un projet engagé qui pourrait mettre en péril financier l'entreprise, ou ne pas répondre aux besoins des opérationnels ; par exemple le développement d'un outil de suivi des conventions avec les spécificités d'un UFR et sans interface avec le logiciel de facturation. Le risque serait d'avoir une convention non tracée et donc de ne pas être en capacité de relancer les financeurs. Une telle situation pourrait générer des impacts importants sur la trésorerie.

Des bonnes pratiques pour limiter les risques :

- Déterminer la tolérance pour le risque de l'institution, en ce qui concerne les SI.
- Définir les stratégies en matière de sécurité de l'information et de gestion des risques des SI.
- Surveiller la mise en oeuvre des stratégies de gestion des risques des SI.
- Comprendre les mandats de conformité et de réglementation.
- S'assurer que les informations sont gérées selon des pratiques efficaces de contrôle de la qualité.
- Collaborer avec les fonctions d'audit informatique et les opérationnels ;
- Etablir des procédures de contrôle des changements des applications;
- Vérifier le cadre de gouvernance des données et la gestion de la sécurité de l'information (confidentialité, classification, etc.);
- Contrôler la planification de la continuité des activités et de reprise après catastrophe.

3.4 Gestion des ressources

Les responsables de la direction informatique gèrent les moyens nécessaires à la mise en place et au bon déroulement des projets ; ils dimensionnent les équipes en fonction des impératifs de production qui doivent être en relation constante avec les services opérationnels concernés afin de répondre à leurs besoins.

Le développement des nouvelles technologies dans la sphère privée conduit les services informatiques à s'adapter aux utilisateurs comprenant et maîtrisant l'informatique, et par conséquent plus exigeants.

Avec l'externalisation, la direction informatique doit piloter les équipes internes et les équipes externalisées en contrôlant la qualité de service et la confidentialité des données au regard du contrat.

A la signature du contrat, la direction informatique a dû s'assurer des recours judiciaires ou financiers possibles et des engagements de service.

Les cadres doivent animer les équipes et veiller à la formation du personnel afin de préserver les talents et de s'adapter à l'évolution des nouvelles technologies ou des nouvelles méthodes de programmation (HTLM par exemple).

Des bonnes pratiques pour limiter les risques :

- Surveiller l'attribution des ressources et la gestion du portefeuille.
- Gérer les actifs informationnels (« hardware et software »).
- Veiller sur les tiers fournisseurs de services ;
- Mettre en oeuvre les normes d'architecture standardisée.
- Gérer le personnel interne et externalisé ;
- Contrôler les budgets opérationnels et d'investissements des SI;
- Vérifier les protocoles de gestion des actifs SI;

3.5 Le pilotage

Le pilotage de la fonction SI vise à examiner les procédures appliquées par le personnel informatique pour l'évaluation des projets, et pour le contrôle de la qualité de la prestation de services.

A titre d'exemple, par un souci de qualité de services, les agents sont informés par mail dès qu'il y a un incident. Ces incidents font l'objet d'analyse et intégré au reporting mensuel de la DSI. Ce type d'organisation et ses méthodes de communication sont développés selon le degré de maturité de la fonction informatique et de sa gouvernance.

Pour la réussite des projets, la DSI (la maîtrise d'oeuvre) doit pouvoir s'appuyer sur les utilisateurs finaux (maîtrise d'ouvrage) qui sont les utilisateurs et les administrateurs fonctionnels des applications déployées. Les activités supports, tels que la direction des ressources humaines et la direction finance) sont moins sensibilisés aux systèmes d'information, alors qui sont les directions qui consolident l'ensemble des données de gestion.

Le sponsor (personne qui sponsorise le projet) est un acteur majeur pour mobilier les équipes support. Il doit évaluer la réussite du projet informatique en intégrant les utilisateurs finaux. Cette évaluation dépend du niveau de maturité de l'administration aux systèmes d'information.

Enfin, le développement des standards informatiques (ITIL, COBIT,…) permettent la mise en place d'indicateurs de comparaison (benchmarking) et le développement d'un référentiel de bonnes pratiques informatiques en interne.

Des bonnes pratiques pour limiter les risques :

- Assurer et mesurer la satisfaction des clients (par exemple, au moyen d'enquêtes par e-mail).
- Maintenir les niveaux de service prévus.
- Évaluer la valeur commerciale de la prestation de services.
- Encourager les initiatives d'amélioration des processus SI.
- Mesurer la gestion du rendement des SI ;

3.6 Conclusion

Pour conclure, une gouvernance efficace se caractérise par la transparence, par la formalisation des travaux, par laprise de décision. Mais aussi, par la capacité de la direction informatique de s'opposer à des éléments qui augmenteraient dangereusement la prise de risques. Si l'une des caractéristiques n'est pas réunie, la gouvernance des systèmes d'information devient fragile.

6 Les liens avec le contrôle Interne comptable et le Contrôle Interne budgétaire

Pour beaucoup l'appellation Contrôle Interne recouvre une réalité financière et comptable. Cette terminologie ne met pas suffisamment l'accent sur la maîtrise des risques qui est à la base même de toute sécurité et protection contre les aléas qu'un organisme peut rencontrer.

Pourtant tout Contrôle Interne doit nécessairement aborder la maîtrise des risques au sens large.

Cet ouvrage est centré sur ce thème et a largement développé le contenu d'une approche par les risques.

Au sein de ce chapitre, il convient de présenter les liens qui peuvent exister entre ces différentes notions : approche par les risques, Contrôle Interne comptable et financier, Contrôle Interne budgétaire.

En effet, nous avons prévu de développer cet angle de vue rarement abordé et qui répond également à différentes interrogations rencontrées par les responsables.

INTRODUCTION ET POSITIONNEMENT DU SUJET

- La détection des risques d'ordre opérationnel doit être le premier élément de construction de toute démarche de Contrôle Interne.

En effet, ces risques sont naturellement majeurs et stratégiques puisqu'ils s'appliquent à des processus opérationnels porteurs du coeur de métier. C'est à ce niveau que se situent les enjeux de performance et de qualité de service, voire d'intérêt vital pour l'entité publique concernée.

La maîtrise des risques opérationnels est une nécessité pour atteindre les objectifs stratégiques, se fixer des ambitions de plus en plus hautes.

Par ailleurs, la survenance de ce type de risque comporte des conséquences financières importantes, quelques fois pouvant remettre en cause l'intérêt public. Leur impact sur les résultats économiques est immédiat.

Ainsi ce premier aspect implique directement la performance, un des objectifs clefs de toute démarche de Contrôle Interne.

Il s'agit d'étendre cette approche par les risques à toutes les fonctions de support, elles-mêmes porteuses de conséquences sur la performance de l'entité.

- Par ailleurs, le Contrôle Interne a pour objectif la production d'informations irréprochables d'ordre budgétaire, comptable et financier et de nature à éclairer la meilleure prise de décision.

Dans ce domaine, la détection et la mise sous tutelle des risques des processus relevant des fonctions comptables et budgétaire sont les premières actions à entreprendre pour construire le Contrôle Interne comptable et budgétaire ; la maîtrise de ces risques est de nature à garantir la sécurité financière et comptable et la qualité de l'information nécessaire à la publication des comptes et à la conduite de la stratégie.

Des normes internationales existent pour garantir la tenue de ces objectifs. Elles sont développées selon les cycles comptables et budgétaires de l'organisme : préparation budgétaire, élaboration budgétaire, exécution des dépenses, exécution des recettes, gestion de la trésorerie, opérations de fin d'exercice.

Néanmoins, on pourrait imaginer de réaliser de manière indépendante et autonome les deux approches :

- D'un côté la gestion des risques opérationnels
- D'un autre côté le Contrôle Interne comptable et budgétaire

… ce tout constituant le Contrôle Interne.

Dans la pratique c'est souvent ce qu'il se passe.

Mais il est dommage de ne pas relier les deux au sein d'une même démarche tant les interactions sont importantes.

Très souvent l'approche des risques opérationnels est déconnectée du Contrôle Interne comptable et financier, étant considérée comme une problématique opérationnelle et non comptable.

Notre propos sera développé selon les deux parties suivantes

1. CE QU'IL Y A EN COMMUN ET QUI RAPPROCHE LES DEUX DÉMARCHES

L'approche par les risques implique nécessairement le Contrôle Interne sur les plans suivants :

- Les risques opérationnels ont un impact financier et sur la performance de l'établissement

- La détection des risques et des aléas apporte à la qualité de l'information comptable une plus grande fiabilité et exhaustivité

- La méthode de détection des risques opérationnels est identique à celle utilisée pour détecter les risques comptables, à savoir basée sur l'analyse des processus.

Les risques opérationnels ont un impact financier et sur la performance de l'établissement

La démarche d'identification des risques opérationnels permet à travers la cartographie des risques de mettre en évidence les situations dans lesquelles un établissement public peut être confronté à une difficulté majeure pour produire ses prestations auprès de ses clients et de la collectivité.

La défaillance de la mission de service public peut être, en effet, source de conséquences d'une très grande ampleur en termes :

- D'image,

- Mais pas seulement, de préjudice important pour le ou les bénéficiaires concernés

- Et finalement financiers pour réparer la situation dégradée.

Ainsi la prudence de gestion suppose donc de savoir correctement analyser les risques, de manière à anticiper les dysfonctionnements potentiels et se mettre en situation de les réduire ou les annihiler.

La détection des risques et des aléas apporte à la qualité de l'information comptable une plus grande fiabilité et exhaustivité

La connaissance des risques auxquels peut être exposé un établissement public est un atout pour savoir établir de manière comptable les provisions pour risques et aléas qui découlent de leur survenance.

Produire un compte financier au plus près de la réalité des risques économiques de l'établissement confère au pilotage économique et à l'appréciation de la performance une plus grande valeur.

En effet, disposer de comptes et d'indicateurs économiques qui anticipent la réalité du terrain est toujours un exercice compliqué à réaliser. Si l'on souhaite éviter les approximations, voire se baser sur des chroniques statistiques pas toujours sûres, l'approche par les risques apportent une précision appréciable.

La méthode de détection des risques opérationnels est identique

La mise en place d'une cartographie des risques passe par une analyse des processus métiers et à travers cette description consiste à mettre en évidence les fragilités de fonctionnement de ces processus. Il convient de faire ressortir les risques qui portent des enjeux forts, d'ordre économique et/ou d'ordre technique.

Il en est de même pour les processus comptables, comme pour toute autre fonction de support de type RH, commercial, achats, …. Il s'agit de mettre à plat également les processus de ces fonctions.

Les démarches sont donc identiques et aboutissent à développer des cartographies de risques adaptées aux spécificités de chaque fonction concernée.

Ainsi développer des approches identiques au sein du Contrôle Interne pour analyser les risques tant opérationnels que comptables permet également d'homogénéiser les pratiques.

2. CE QUI EST SPÉCIFIQUE AU CONTRÔLE INTERNE COMPTABLE ET BUDGÉTAIRE

Une mission prégnante et commune à l'ordonnateur et au comptable est de garantir la qualité de l'information financière.

Ainsi, les budgets et comptes financiers se préparent-ils ensemble. Cependant, les documents imposés par les règlements, aussi

complets puissent-ils être, ne permettent pas, du fait de leurs caractéristiques métiers, d'être facilement appréhendés par les administrateurs. Ces-derniers disposent de délais restreints et ne sont pas au coeur du métier, compte-tenu de leur position particulière au sein des organismes publics. La confiance dans l'information financière est donc primordiale. La confiance n'exclut pas le contrôle dont sont chargés les contrôles budgétaires publics, la Cour des comptes et les corps d'inspection qui sont les autres destinataires des informations budgétaires et comptables.

C'est dans ce contexte que le Contrôle Interne budgétaire et comptable trouve toute sa place et sa spécificité.

Si les contrôles budgétaire et comptable reposent sur des bases communes de régularité, sincérité, exactitude, exhaustivité, il n'en demeure pas moins que la soutenabilité budgétaire qui repose sur le seul ordonnateur présente des spécificités en-dehors des aspects purement comptables. Ainsi en est-il la qualité de la programmation budgétaire, de son suivi et de son actualisation. Cependant, une articulation et, d'une manière plus pragmatique, un réel travail d'équipe entre l'ordonnateur et l'agent comptable sont les garants d'une soutenabilité budgétaire optimale.

A cet égard on peut regretter que la prestation de serment par l'agent comptable ne trouve pas son équivalent pour l'ordonnateur dans la mesure où la solennité de cette prestation, au-delà de son aspect purement formel, permettrait aux uns et aux autres de se présenter devant le juge financier avant le contrôle et par là de prendre la mesure du rôle et des responsabilités de l'ordonnateur, celles de l'agent comptable étant d'emblée connues et reconnues par tous.

3. LES APPORTS DU DÉCRET GBCP

Par ailleurs, il est important de rappeler que le Contrôle Interne comptable et budgétaire reste une des priorités des démarches de performance que l'Etat souhaite mettre en oeuvre, notamment pour appuyer la réforme budgétaire introduite par le décret GBCP.

En effet, plus de 700 établissements publics sont concernés par la réforme du cadre budgétaire. Et d'autres entités publiques, telles que les collectivités locales, seront certainement impliquées par cette réforme demain.

Le décret no 2012-1246 du 7 novembre 2012 développe effectivement au sein des articles 170 et 215 la nécessité de déployer un CI budgétaire et un CI comptable au sein de chaque ministère et organisme public.

« Le Contrôle Interne budgétaire a pour objet de maîtriser les risques afférents à la poursuite des objectifs de qualité de la comptabilité budgétaire tenue et de soutenabilité de la programmation et de son exécution.

Le Contrôle Interne comptable a pour objet la maîtrise des risques afférents à la poursuite des objectifs de qualité
des comptes depuis le fait générateur d'une opération jusqu'à son dénouement comptable. »

S'il mentionne l'importance de la mise en place de dispositifs de Contrôle Interne, le décret GBCP apporte également, en matière de pilotage budgétaire, des avancées considérables qui permettent de mieux anticiper les charges des organismes publics, et par voie de conséquence d'optimiser la performance.

La mise en application des dispositions de ce décret est donc de nature à renforcer la capacité des gestionnaires à diriger leur établissement. Son accompagnement par un dispositif de Contrôle Interne sera également un prérequis pour assurer l'optimisation des instruments de pilotage.

4. LES APPORTS DU DÉCRET GBCP

LDevoir d'alerte de l'agent comptable :
Les agents comptables ont un devoir d'alerte formalisée par l'Instruction n°NOR BCRZ1000060J du 6 août 2010 relative au devoir d'alerte dans le secteur public local : qui leur fait « obligation de signaler à leur hiérarchie non seulement des infractions pénales et des illégalités constatées dans l'exercice de leurs fonctions mais également des dérives de gestion », c'est-à-dire la faute de gestion et la gestion de fait.

Ainsi, « Les faits de nature à déclencher une alerte sont ceux qui sont susceptibles de constituer soit une infraction (c'est à dire une violation de la loi), soit une dérive de gestion des organismes publics. »

En aucun cas contrôle d'opportunité de la part des agents comptables
Il convient de préciser que la dérive de gestion ne s'apprécie pas en opportunité : l'agent comptable n'est pas juge

de la légalité et de l'opportunité des décisions de l'ordonnateur, ce qui ne lui interdit pas de faire part de ses soupçons. Ce rôle doit s'entendre dans le cadre d'une collaboration entre l'ordonnateur et le comptable, ce dernier mettant en garde l'ordonnateur sur la dangerosité de pratiques, dont, de bonne foi, il n'aurait pas conscience.

En outre, ce devoir d'alerte permet une meilleure articulation de l'agent comptable avec les organismes de contrôle.

Possibilité que l'agent comptable soit chef des services financiers

L'article 188 du décret n°2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique (GBCP) dispose que l'agent comptable peut exercer, à la demande de l'autorité exécutive de l'organisme, des fonctions de chef des services financiers.

Dans ce cadre, l'ordonnateur peut lui confier le suivi des crédits budgétaires, de la liquidation de l'émission de ordres de recettes et de la tenue de la comptabilité des autorisations d'engagement.

Il y a lieu de s'interroger a priori sur la compatibilité de cette possibilité avec le principe de la séparation de l'ordonnateur et du comptable.

La réponse tient au fait que la compatibilité est assurée dans la mesure où l'agent comptable, en tant que chef des services financiers, n'engage ni n'ordonne jamais la dépense (il ne signe pas d'engagement juridique tels que bon de commande, subvention, convention) et ne recrute jamais de personnel (il n'est pas signataire du contrat de travail). Il n'est pas non plus compétent pour certifier le service fait.

Ce chapitre souligne une fois de plus, non seulement la nécessité du travail d'équipe entre l'ordonnateur et le comptable, mais aussi son intérêt aussi bien pour le Contrôle Interne, afin d'assurer la qualité de l'information budgétaire et comptable, que pour leurs fonctions respectives dans un environnement d'utilisation rationnelle, sûre et pragmatique des financements publics.

5. CONSÉQUENCES ET ENJEUX DU CONTRÔLE INTERNE

Le renforcement des dispositifs de Contrôle Interne et d'audit interne répond à la nécessité de mieux gérer sur le plan économique les établissements publics.

Déjà un grand nombre d'entre eux bénéficie de démarches de certification des comptes menées par des commissaires aux comptes qui ont permis de solidifier les instruments de pilotage économique.

Le Contrôle Interne est un outil qui a pour objet d'améliorer l'information comptable, mais également de favoriser l'efficacité économique.

En effet, les enjeux sont de réduire les dépenses tout en assurant la meilleure qualité de service. Ces deux objectifs facilement antagonistes constituent des challenges incontournables pour les établissements publics. La réduction des dépenses de l'état et des organismes publics passe par une optimisation des processus et une capacité d'anticipation des risques que le Contrôle Interne a pour objet de favoriser.

CONCLUSION

Nous espérons que ce document aura permis au lecteur d'avoir pu préciser son opinion sur le contrôle interne.

A la fois, méthodologie, expérience partagée, connaissances des organisations publiques et de leurs métiers constituent des points d'appui sur lesquels il convient de partir pour développer une démarche de contrôle interne.

Les différents contributeurs à la réalisation de ce livre blanc ont pu apporter leur valeur ajoutée dans ces différentes dimensions. L'aspect pratique et opérationnel a été privilégié et a servi de base aux développements de ce sujet.

A ce titre nous remercions chaleureusement tous les participants pour la qualité de leurs apports.

Groupe Services Publics

Contactez-nous
Valérie SAINT-YVES
valeriesaintyves@dfcg.asso.fr
14 rue Pergolèse
75016 Paris
Tél. : 01 70 36 34 93
Fax : 01 42 27 04 03

ASSOCIATION NATIONALE
DES DIRECTEURS FINANCIERS
ET DE CONTRÔLE DE GESTION

www.dfcg.fr
www.dfcg-news.com