Vendredi
12|10

Conseil Départemental de la Haute-Garonne

Ateliers thématiques

CIAT 9e 2018

Conférence des Inspecteurs et Auditeurs Territoriaux

L'AUDIT INTERNE

Acteur de progrès éthique et de modernisation 3.0 dans les collectivités territoriales

ciat

ifaci

AMRAE

HG
CONSEIL DÉPARTEMENTAL HAUTE-GARONNE.FR

Ateliers Thématiques

SOMMAIRE

Atelier thématique :

Atelier COSO N°1 :

"GOUVERNANCE ET CULTURE : quels enjeux ?"

Animateurs :

- **Agnès BACHELOT-JOURNET**
  Directrice de la Performance et Modernisation du Service Public
  Conseil Départemental Isère

- **Hélène MATHIEU**
  Directrice Générale de l'Inspection Générale
  Ville de Paris

I. Principe 1 : exercer une surveillance des risques par le Conseil

1. *Les questions à se poser*

Sur la définition du « Conseil », il y aura sans doute autant de modèles que de collectivités, il convient donc de s'interroger sur qui participe à ce conseil (élus –majorité et/ou opposition, DG…).

2. *Les écueils à éviter*

- Attention à la différence entre :
  - Le comité des risques qui est opérationnel
  - Le comité d'audit qui doit être indépendant
- La cartographie des risques doit être équilibrée entre les risques politiques (liés au programme de mandature) et les risques plus opérationnels (continuité du service public) qui peuvent faire l'objet d'un programme « incompressible » d'audits.

3. *Les bonnes pratiques*

Pour favoriser l'appropriation de la culture du risque par les élus, donner des exemples très concrets d'impact comme les risques pénaux. Exemple : annulation de l'élection d'un maire qui avait utilisé une photo de la photothèque de la mairie pour son dépliant électoral.

4. *Des exemples dans les collectivités pour accroître l'implication des élus*

- Ville de Paris :
  - les élus de l'opposition proposent des thèmes d'audit qui sont intégrés dans le programme, ce dernier étant validé in fine par l'exécutif.
  - Le plan de mandat est clair, ce qui permet, en creux, de bien définir les risques, soit la non-atteinte des objectifs du plan de mandat.
- Ministère des armées : les risques posés doivent répondre aux intérêts du top management. Le comité des risques est donc porté par le comité exécutif qui comprend les responsables de l'ensemble des grands corps d'armée.

II. Principe 2 : définir les structures organisationnelles

1. *Les questions à se poser*

- La comitologie doit s'adapter à la taille de la collectivité
- La loi Sapin 2 est une bonne opportunité et un accélérateur pour mettre en place un comité des risques qui, s'il ne comprend pas forcément des élus, doit leur rendre compte.
- Aujourd'hui les outils de contrôle pour les collectivités territoriales ne sont pas en rapport avec l'importance de leurs budgets (a contrario des obligations qui pèsent sur les entreprises) tandis que les usagers/citoyens souhaitent bénéficier d'outils de surveillance de l'argent public.

2. *Les écueils à éviter*

Multiplier des indicateurs « rassurants », mais inutiles, plutôt que de se focaliser sur quelques indicateurs qui permettent de piloter les objectifs stratégiques.

3. *Les bonnes pratiques*

- Accepter de mettre en place ce processus par tâtonnement plutôt que d'être paralysé par un idéal inatteignable.
- Avoir des recommandations concrètes et réalistes.

III. Principe 3 : attirer, définir la culture souhaitée

1. ***Les écueils à éviter***
   Afficher des valeurs en contradiction avec le programme de la mandature, manquer de cohérence.

2. ***Les bonnes pratiques***
   - Les valeurs de la collectivité doivent transcender la mandature
   - Ces valeurs doivent être retranscrites de manière très opérationnelle.

IV. Principe 4 : démontrer l'engagement en faveur de valeurs fondamentales (intégrité et éthique)

1. ***Les questions à se poser***
   Quelle communication au grand public de la cartographie des risques ? Il s'agit ici d'un sujet majeur de la démocratie.

2. ***Les bonnes pratiques***
   L'exemplarité.

V. Principe 5 : attirer, former et fidéliser des personnes compétentes

1. ***Les écueils à éviter***
   - Veiller aux incompréhensions entre élus et administration du fait du décalage de temporalité : temps politique versus continuité du service public.
   - Le turn over des équipes peut générer une perte de connaissance sur les risques.

2. ***Les bonnes pratiques***
   - Garantir le tuilage.
   - Faute de pouvoir proposer des salaires importants, l'administration pourra mettre en avant les valeurs du service public.

Atelier thématique :

Atelier COSO N°2 :

"STRATEGIE ET DEFINITION DES OBJECTIFS : comment définir l'appétence d'une collectivité pour le risque et définir des stratégies et objectifs opérationnels ?

Animateurs :

- **Stéphane LABONNE**
  Mission d'Inspection Générale
  Conseil Régional des Pays de la Loire

- **Charles-Thibault PETIT**
  Inspecteur Général
  Conseil Départemental de l'Essonne

Atelier COSO n° 2

Stratégie et définition des objectifs : comment définir l'appétence d'une collectivité pour le risque et définir des stratégies et objectifs opérationnels ?

Intervenants :

- Charles-Thibault PETIT - Inspecteur général - Conseil départemental de l'Essonne
- Marie-Christine DE GOURNAY - Chef de l'audit - Conseil départemental de l'Isère
- Stéphane LABONNE - Inspection générale - Région des Pays de la Loire
- Axelle BRAULT-FONTERS - Associée Risk Management - Grant Thornton

IX^{ème} Conférence des inspecteurs et auditeurs territoriaux

Toulouse - 12 octobre 2018

Fondements et enjeux

Stratégie et définition des objectifs est l'une des cinq composantes du COSO ERM (Enterprise Risk Management) 2017

Le management des risques de l'entreprise - Source : COSO 2017

Les quatre autre composantes du COSO ERM 2017 sont :

- gouvernance et culture;
- performance;
- Revue et amendement;
- information, communication et reporting.

Ces 5 composantes sont divisées en 20 principes.

Fondements et enjeux

Qu'est-ce que le COSO-ERM 2017 ?

Le COSO ERM 2017 s'inscrit dans la continuité du COSO 2 (2004).

Il prend acte :

- de l'émergence de nouvelles menaces et opportunités liées à la marche accélérée de l'économique numérique (Big Data, cybersécurité…) ;
- de l'irruption de nouveaux risques d'image liées à des exigences accrues en matière de déontologie et d'éthique;
- de la part grandissante du risk management dans les modèles de gouvernance .

Il repose sur les principes suivants :

- prise en compte de la culture d'entreprise et des valeurs éthiques comme paramètre de la gestion de risques;
- intégration de la gestion de risques dans la définition et le suivi de l'exécution de la stratégie;
- cohérence de la gestion de risques avec l'atteinte des objectifs de performance.

Attention

Il convient de distinguer le COSO-ERM du **COSO Contrôle interne** dont la dernière mise à jour date de 2013. Ces deux textes sont complémentaires mais ne couvrent pas les mêmes champs; ils sont donc actualisés séparément.

Présentation de la composante Stratégie et définition des objectifs

Finalité

Comment décliner avantageusement à votre collectivité cette composante du COSO ERM ?

Composition

La composante comprend 4 principes qui sont successivement mis en œuvre :

- Principe 6 - Analyser le contexte de l'organisation
- Principe 7 - Définir l'appétence pour le risque
- Principe 8 - Evaluer les stratégies alternatives
- Principe 9 - Définir les objectifs opérationnels

Qui ?

L'exercice concerne prioritairement l'Exécutif de la collectivité, la direction générale et le risk manager (s'il existe)

Quand ?

L'exercice doit être répété dans son intégralité :

- en début du mandat
- à mi-mandat afin de réactualiser l'analyse menée
- en fin de mandat pour un bilan et préparer le mandat suivant

Et pour autant que nécessaire, notamment en cas de modification significative des éléments de contexte et/ou du projet de mandat

Principe 6 Analyser le contexte de l'organisation

Objectif

Analyser les impacts potentiels du contexte dans lequel la collectivité évolue afin d'en déduire des incidences sur sa capacité à atteindre les objectifs qu'elle s'est fixés, qui sont en lien avec sa mission, sa vision et ses valeurs fondamentales

Points d'attention

- Déterminer les éléments de contexte externes et leurs influences
- Déterminer les éléments de contexte internes
- Anticiper les facteurs majeurs qui pourraient avoir des impacts sur les résultats attendus
- Identifier les parties prenantes dont dépend la réalisation des activités de la collectivité

Livrable

- Rapport en assemblée délibérante
- Restitution en comité de direction

Aller plus loin…

- Mener à bien un benchmarking des collectivités comparables
- Réaliser ces travaux en lien avec un observatoire ou toute instance dédiée à la réflexion prospective

Principe 7 Définir l'appétence pour le risque

Objectif

Définir le niveau de risque acceptable et identifier les risques que la collectivité est prête à prendre, du fait de leur faible criticité et/ou parce qu'assumer ce risque permet d'atteindre plus facilement un objectif fondamental du mandat [suite du principe 6]

Points d'attention

- Nécessité d'outils pour l'objectiver (cartographie des risques, matrice coûts/avantages…) ainsi qu'un recensement précis des moyens de contrôle interne existants
- Cette appétence doit être arbitrée au plus haut niveau décisionnel
- Elle aide à conforter la stratégie globale, calibrer les objectifs stratégiques puis les actions concrètes et doit faire l'objet d'une communication interne
- Utiliser avec prudence la notion de tolérance au risque

Livrable

Décision formalisée par une consultation *ad hoc* de l'Exécutif (président ou Exécutif collégial, par exemple réunion de majorité)

Aller plus loin…

- Faire de cette démarche un processus décisionnel structurant de la collectivité, éventuellement en créant un comité dédié (comité des risques)
- Utiliser les missions d'audit pour réexaminer la criticité des risques et ajuster en conséquence le périmètre d'appétence

Principes 8 & 9 — Evaluer les stratégies alternatives
Définir les objectifs opérationnels

Objectif

Après examen des différents *scenarii* possibles, mettre en place un cadre opérationnel pour la réalisation des objectifs de la collectivité en cohérence avec le niveau de risque accepté (principe 7) et le coût acceptable des mesures de maîtrise requises

Points d'attention

- Pour chaque stratégie étudiée, analyser le profil de risques et évaluer le coût des mesures de maîtrise envisagées
- La méthode retenue doit intégrer les évolutions extérieures susceptibles d'affecter l'atteinte des objectifs de la collectivité (cf. principe 6)
- Revoir les moyens alloués pour les concentrer sur les objectifs prioritaires, au regard de l'importance du travail à mener en termes de réduction du risque net (démarche de type MARCI)
- Une fois qu'une stratégie est adoptée, mettre en place un système de suivi de l'évolution des critères pris en compte avec une attention particulière au suivi du coût des mesures de maîtrise

Livrable

Note au DG formalisant la méthode et objectivant les choix réalisés et arbitrage subséquent

Aller plus loin…

Adapter les systèmes de veille informationnelle interne et externe pour y intégrer les risques émergents susceptibles de remettre en cause la pertinence de la stratégie retenue

Questions-réponses

Atelier thématique :

Atelier COSO N° 3 :

"PERFORMANCE :
comment développer au sein d'une collectivité une vision globale des risques :
identification, niveau de criticité, et priorisation ?"

Animateurs :

- **Christophe MAGNE**
  Directeur de l'Audit Interne
  Conseil Départemental Haute-Garonne

- **Guillaume PARADAS**
  Directeur de l'Audit et des Risques
  Conseil Régional Auvergne Rhône Alpes

COSO ERM

Composante « Performance »

Développer une vision globale des risques en collectivité

IX^{ème} CIAT
Toulouse – 12 octobre 2018

Channez KRIM
Christophe MAGNE
Guillaume PARADAS

Déroulement de l'atelier :

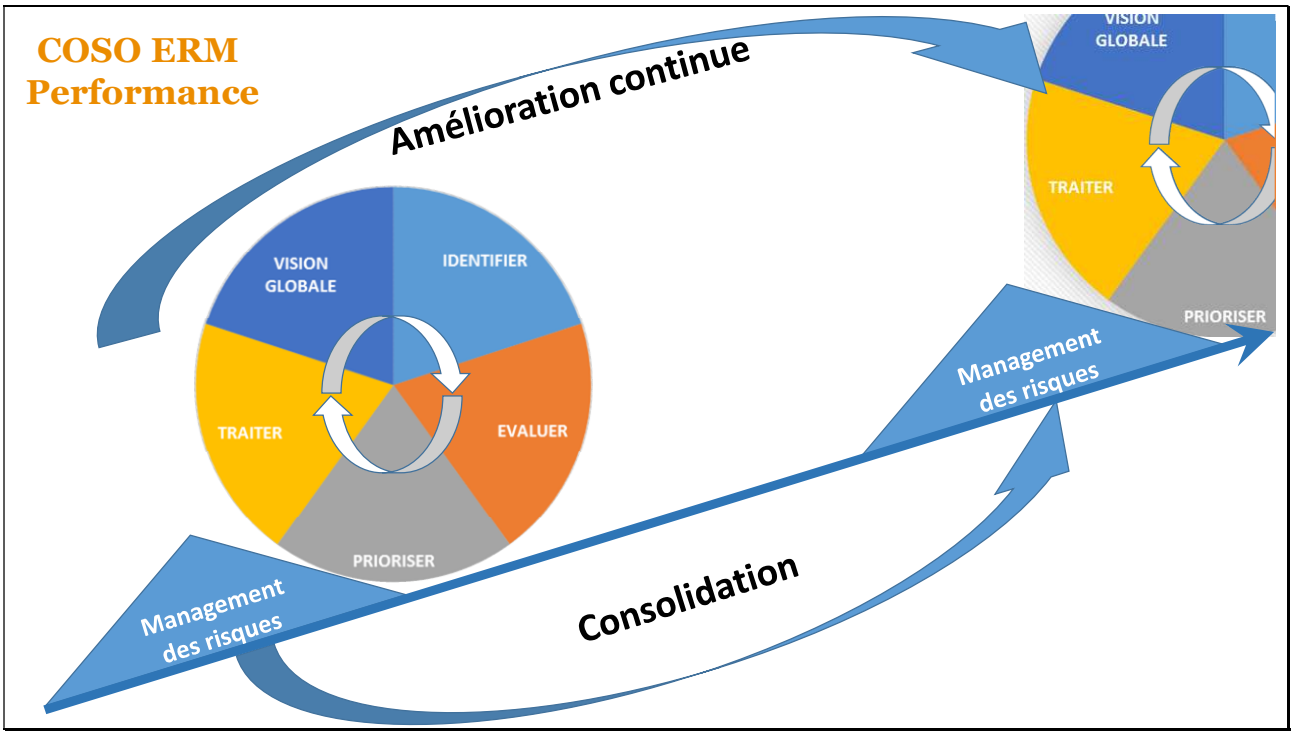
- **4 temps pour cet atelier :**

1. Temps 1 : en plénière: présentation de la démarche, des principes, définitions, modalités pratiques - 20 mn max;
2. Temps 2 : travail en 2 groupes : désigner des rapporteurs, un sous groupe liste des écueils a éviter, un sous groupe liste des astuces et bonnes pratiques - 20mn
3. Temps 3 : partage en plénière : présentation des rapporteurs - 10mn
4. Temps 4 : en plénière: debrief global par les animateurs, éventuellement vote sur une ou deux bonnes pratiques (proposées par les animateurs pour éviter un écueil resté sans solution, ou ayant fait débat dans le sous groupe dédié).

- **Evaluation :**

1- Qu'est ce qui a particulièrement retenu votre attention au cours de l'atelier?

2- Avec quoi vous repartez d'utile à vos pratiques ?



COSO ERM - Performance

Principe 10 : Identifier les risques

- L'organisation s'engage à recenser les risques de toute nature pesant sur (ou générés par) les activités qu'elle met en œuvre en déclinaison de sa stratégie et susceptibles d'entraver l'atteinte de ses objectifs

Questions à se poser

- Qu'est-ce qu'un risque? Quelle typologie de risques retenir? Quelles sont les activités / objectifs les plus concernés?
- Quelle méthode permettrait d'optimiser le recensement? Comment expliquer les concepts et la démarche aux parties prenantes rencontrées?
- Est-ce que la démarche est portée au bon niveau?
- Parmi les informations qui vont être collectées dans le courant de la démarche, lesquelles seront à considérer comme confidentielles?
- Sur quels documents, bases de données, etc. est-il possible de s'appuyer au démarrage et dans le courant de la démarche?
- Quel niveau de qualité et de complétude du recensement des risques est-il possible d'atteindre? Faut-il adapter l'ambition ou la méthode?

Pour débuter la mise en œuvre :

- Cadre méthodologique simple / définitions intelligibles par tous / outillage souple / planning réaliste
- Détermination du périmètre: activités / processus / ressources sur lesquels on s'attend à trouver les principaux risques
- Identification des objectifs de la collectivité potentiellement concernés (obligations légales /règlementaires, plan de mandat, etc.)
- Exploitation de la documentation existante pour un 1er recensement (rapports d'audit interne et externe, bilan des rejets Paierie, etc.)
- Lettre de mission du commanditaire ciblée sur les attendus, la méthodologie, le calendrier et communication interne aux contributeurs
- Faire arbitrer dès le début de la démarche les règles relatives à la diffusion des productions / communicabilité des résultats

Modalités pratiques d'application au secteur public

- Capitaliser sur l'existant (conclusions CRC, jurisprudence, sinistralité, procédures disciplinaires, rapports d'audit interne, etc.)
- Convaincre la DG et sensibiliser l'Exécutif pour un double portage politique et hiérarchique de la démarche
- Mener la démarche avec un haut degré de confidentialité
- Associer les organismes satellites/tierces parties

Pour aller plus loin :

- Approche transversale: (re)placer les risques dans la cartographie des processus (identifier les étapes critiques dans les processus clés)
- Lorsque la méthode a gagné en maturité dans l'organisation, recourir à des ateliers collaboratifs croisant plus largement les appréciations

COSO ERM - Performance

Principe 11 : Evaluer la criticité des risques

- L'organisation s'engage à mesurer et réévaluer régulièrement la criticité (occurrence et gravité) de l'ensemble de ses risques par une méthode rigoureuse, constante, adaptable, suffisamment simple et produisant des résultats assez pertinents pour être mobilisatrice et partagée.

Questions à se poser

- La méthode est-elle adaptable à tout type de risque / d'activité? Produira-t-elle des indicateurs pertinents pour tous les niveaux?
- Est-ce que tous les contributeurs ont eu connaissance de la démarche d'identification et des attendus de l'évaluation?
- Est-ce qu'un risque critique pour l'activité ou l'entité concernée, l'est également à l'échelle de l'organisation? Est-ce que certains risques sont critiques pour la collectivité, même s'ils ne le sont directement pour aucune entité en particulier?
- Des risques similaires identifiés par plusieurs directions sont-ils corrélés? Peuvent-ils se réaliser simultanément?

Pour débuter la mise en œuvre :

- Formaliser et valider la méthode, les objectifs généraux, les livrables attendus, les moyens à mobiliser, le calendrier et les échéances.
- Communiquer en amont sur la démarche et la méthode et présenter la forme des produits finis (modèles de tableaux de bord et de matrices).

Modalités pratiques d'application au secteur public

- Echelles simples et sans valeur médiane
- Un même risque présentant plusieurs impacts se cote au niveau de l'impact le plus dommageable à l'atteinte des objectifs
- Distinguer les risques bruts (théoriques) et les risques nets (constatables)
- Exploiter l'information disponible sur les faits avérés : incidents de gestion, sinistralité, contentieux, AT-MP et IPP, fraudes, etc.
- Exploiter les évaluations des risques antérieures à la démarche (rapports d'audit, etc.) avant de recourir à l'estimation des acteurs
- Prendre en compte l'impact des risques en termes de réputation de la collectivité et de ses dirigeants
- Associer les partenaires / satellites à l'évaluation des risques que la collectivité partage avec eux ou qu'elle est susceptible d'« importer »

Pour aller plus loin :

- Lorsque la méthode a été partagée et éprouvée par les réévaluations, affiner les échelles et y adjoindre une cotation des contrôles existants.
- Réévaluer hors cycle les risques concernés par une évolution du contexte ou de l'appétence, une variation dans les indicateurs clés, etc.
- Insérer la démarche dans un processus permanent: proposer des tableaux de bord, des réévaluations, etc. en s'appuyant sur un outil dédié
- Evaluer les risques cibles compte-tenu des risques jugés acceptables par la gouvernance (plans d'actions post-audit, marges d'amélioration);
- Pour les risques exogènes rares mais susceptibles d'avoir des impacts extrêmes sur l'organisation, recourir à des analyses par scénario

COSO ERM - Performance

Principe 12 : Prioriser les risques

- Sur la base de la cartographie, l'organisation s'engage à déterminer les risques dont elle attend une amélioration substantielle et mesurable du niveau de maîtrise (détermination du risque cible), en vue d'élaborer une stratégie et un plan d'action

Questions à se poser

- De quelles informations a besoin la gouvernance pour se prononcer sur la priorisation des risques?
- La volonté politique et les engagements pris ont-ils été suffisamment pris en compte pour prioriser les risques ?
- A-t-on pris suffisamment en compte les aspects déterminants avancés par les managers opérationnels pour prioriser les risques ?
- Est-ce que les priorités sont redescendues au niveau du management opérationnel?

Pour débuter la mise en œuvre :

- Déterminer qui est légitime pour prioriser les risques; organiser et animer la gouvernance en conséquence.
- Entendre la gouvernance sur son appétence au risque et sur les informations / indicateurs qu'elle estime nécessaires pour arbitrer les priorités

Modalités pratiques d'application au secteur public

- 5 critères permettent de hiérarchiser les risques: l'adaptabilité de l'organisation, la complexité du risque ou de ses impacts, la vélocité du risque, la persistance des effets et la résilience de l'organisation
- La priorisation des risques doit prendre en compte la hiérarchisation des objectifs et activités correspondantes, et celle des processus
- Les risques pointés par les organes de contrôle externes (CRC, etc.) sont prioritaires, indépendamment de leur cotation
- Des ateliers d'échanges entre propriétaires de risques permettent de dépasser les biais subjectifs
- L'évaluation et la priorisation des risques peut se faire ex-ante, par exemple lors de la conception ou de la révision d'une politique publique, d'un dispositif, d'une action ou d'un projet

Pour aller plus loin :

- En parallèle de la priorisation des risques (nets), établir une analyse objectivée des marges d'amélioration de la maîtrise (simplification des processus, optimisation des ressources, identification de « *quick wins* »)

COSO ERM - Performance

Principe 13 : Mettre en œuvre les modalités de traitement des risques

- Sur la base de la priorisation, la gouvernance détermine une ou des stratégies de maîtrise des risques, déclinables en mesures de traitement adaptées et proportionnées (acceptation, évitement / suppression, augmentation, réduction ou partage / transfert du risque)

Questions à se poser

- Interroger la Gouvernance, pour chaque risque prioritaire, sur son choix entre acceptation, évitement, augmentation, réduction ou partage. Le cas échéant, lui proposer également une révision des objectifs, de la stratégie ou l'élévation de son niveau d'acceptabilité du risque
- S'interroger sur le rapport entre criticité et priorité accordée au risque d'une part, et ampleur et coûts des mesures de traitement d'autre part.
- Quel support pour le suivi des modalités de traitement? Quel *reporting* à la DG / Exécutif? Comment mesurer les effets?
- Quand est-ce qu'un risque devient acceptable : quand les modalités de traitement parviennent à réduire au niveau cible sa criticité ou lorsque, malgré la mise en œuvre des mesures de traitement, il demeure des facteurs sur lesquels on ne peut agir?
- Se demander à quel moment on peut considérer qu'un risque est éteint: quand les modalités de traitement parviennent à réduire sa criticité résiduelle au minimum ou lorsque celle-ci resterait au minimum même en l'absence de dispositif de maîtrise?

Pour débuter la mise en œuvre :

- Disposer d'éléments objectifs évaluer le dispositif de maîtrise existant et les marges d'amélioration
- Avoir connaissance des plans d'action en cours et des effets attendus sur la maîtrise des risques avant de décider de mesures nouvelles

Modalités pratiques d'application au secteur public

- Les mesures de traitement des risques prioritaires doivent prévoir la répartition des rôles attendus, ne doivent pas aboutir à des non-conformités règlementaires, doivent être documentés, peuvent nécessiter d'impliquer des acteurs externes à l'organisation, peuvent donner lieu à information ou avis d'instances consultatives
- Lorsque est décidé d'augmenter la couverture d'un risque ou de transférer un risque émergeant, il faut s'interroger sur l'opportunité d'anticiper les échéances de renégociation des contrats s'assurance en cours.
- La mise en œuvre des plans d'action approuvés par la Gouvernance doit faire l'objet d'un suivi et d'un *reporting*

Pour aller plus loin :

- Revues de mise en œuvre impliquant à la fois la Gouvernance, les 2 premiers niveaux de maîtrise et le conseil sur les risques
- Actualisation régulière des cartographies de risques pour tenir compte des effets des mesures de traitement sur les risques résiduels et, le cas échéant, identifier les risques nouveaux générés par les mesures de traitement elles-mêmes

COSO ERM - Performance

Principe 14 : Développer une vision globale du portefeuille de risques

- L'organisation s'engage à adosser son management des risques à son pilotage stratégique en donnant à sa gouvernance une vision d'ensemble du portefeuille des risques soutenant la répartition des responsabilités et la prise de décision

Questions à se poser

- Quelles sont les attentes de la gouvernance en terme de vision des risques (exhaustivité, criticité, périodicité d'actualisation, etc.)?
- Comment concilier les impératifs d'exhaustivité et de clarté de la vision des risques?
- Comment faire de la vision globale du portefeuille de risques un réel support à la prise de décision?
- Comment faire converger le pilotage stratégique et le management des risques?
- Quelle méthodologie permet d'aboutir à une gestion de portefeuille passant aisément d'un suivi en rythme de croisière à un suivi rapproché?

Pour débuter la mise en œuvre :

- Entendre la Gouvernance sur son besoin de *reporting* et sur les objectifs que la collectivité souhaite particulièrement prémunir des risques
- Connaître les indicateurs « obligatoires » ou donnant lieu à un *reporting* régulier, afin d'identifier les indicateurs de risques à bâtir en vis-à-vis
- Lier l'organisation et le portefeuille de risque pour identifier les responsabilités en termes de suivi, d'actualisation et de *reporting*.

Modalités pratiques d'application au secteur public

- Lier le calendrier d'actualisation des indicateurs de risque à l'annualité budgétaire et autres grands rendez-vous; rattacher les indicateurs de risques aux politiques publiques et aux principaux processus ressources pour bonne appropriation par l'Exécutif et la DG
- Bâtir des indicateurs de risques en vis-à-vis d'indicateurs « obligatoires » déjà produits et suivis par la collectivité
- Lier les indicateurs de risque les uns aux autres en reconstituant les chaînes de causalité pour agir sur les causes premières ou en curatif
- L'approche peut être centrée sur l'analyse des risques majeurs par service ou sur l'analyse des risques majeurs à l'échelle de la collectivité. Elle peut être représentée en indiquant la typologie et l'évaluation des risques par rapport au niveau cible, en faisant ressortir les risques dont la criticité augmente à mesure de leur consolidation à des niveaux plus élevés (ou l'inverse), voire des risques compensant d'autres risques

Pour aller plus loin :

- Cartographies des risques par processus, par objectifs, etc.
- Etablir une base comparative (benchmarking interne voire externe)
- Simulation d'occurrence de risques extrêmes référencés dans le portefeuille et évaluation des capacités d'adaptation et de résilience.

Atelier thématique :

Atelier AFA :

"Comment mettre en œuvre un code de conduite anti-corruption et un dispositif d'alerte interne ?"

Animateurs :

- **Caroline CALBO**
  Inspectrice Générale des Services
  Conseil Régional Nouvelle Aquitaine

- **Catherine LIOTTIER**
  Responsable Audit Interne
  Conseil Départemental Manche

IX^{ème} Conférence des inspecteurs et auditeurs territoriaux

12 octobre 2018 - Toulouse - CD Haute-Garonne

ATELIER AFA

Comment mettre en œuvre un code de conduite anticorruption et un dispositif d'alerte interne

Intervenants :

- Caroline CALBO - DGS Région Nouvelle-Aquitaine
- Catherine LIOTTIER - Responsable Audit, Mission Audit, Risques et Conformité - Département de la Manche
- Alexandre DE GRENIER DE LATOUR - Auditeur interne - Direction de l'Audit, du Contrôle Interne et de la Gestion des risques - Département de Seine-Saint-Denis

Objectif de l'atelier :

Répondre ensemble aux interrogations que soulève la mise en œuvre d'un programme anticorruption

A partir des travaux CIAT/IFACI sur les recommandations de l'AFA

- Fiche recommandation 2 - Code de conduite anticorruption
- Fiche recommandation 3 - Dispositif d'alerte interne

à partir de vos remarques sur ces fiches

à partir de vos expériences,

ou de vos pages blanches ! …

Les recommandations de l'AFA… qu'est-ce que c'est ?

En décembre 2017, sur le fondement de l'article 3-2 de la loi du 9 décembre 2016 (Loi Sapin II) l'Agence française anticorruption (AFA) a publié un ensemble de recommandations concernant la détection et la prévention des risques de fraude.

Pour les collectivités territoriales, ces recommandations sont ainsi déclinées :

- Engagement des instances dirigeantes ;
- **Code de conduite anti-corruption ;**
- **Dispositif d'alerte interne ;**
- Cartographie des risques de corruption ;
- Procedure d'évaluation des tiers ;
- Procédure de contrôle comptable;
- Dispositif de formation au risque de corruption;
- Dispositif de contrôle et d'évaluation interne .

Avis relatif aux recommandations de l'Agence française anticorruption (…)
JORF n°0298 du 22 décembre 2017

Présentation des Fiches AFA

Recommandation n° 2 - Code de conduite anticorruption

Le code de conduite anticorruption est une matérialisation de la volonté de la collectivité de s'engager contre la corruption, dans une démarche comprenant prévention et détection des faits. Clair et précis, il ne doit pas laisser place à l'ambivalence ou être sujet à interprétation.

« Le code de conduite anticorruption (quelle que soit la dénomination retenue par l'organisation en pratique) manifeste la décision de l'instance dirigeante d'engager l'organisation dans une démarche de prévention et de détection des faits de corruption. Il est clair, sans réserve et sans équivoque.

Il recueille les engagements et principes de l'organisation en cette matière.

Il définit et illustre les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption. »

Extrait de la recommandation AFA n° 2

Présentation des Fiches AFA

Recommandation n° 2 - Code de conduite anticorruption

Contenu du Code de conduite

- Il rappelle les valeurs et engagements de la collectivité sur la prévention mais aussi la détection des faits de corruption.
- Il décrit les situations que peuvent rencontrer les agents et relevant de la corruption.
- Il contient une description des comportements à respecter lors des situations à risque.
- Il présente la liste des interdictions à observer, notamment au sujet du mécénat, des cadeaux, des invitations, des conflits d'intérêts et paiements visant à faciliter l'obtention d'avantages.
- Il prévoit les sanctions disciplinaires encourus par l'agent enfreignant les engagements et principes de la collectivité.
- Il présente le dispositif d'alerte interne, que les agents peuvent suivre pour effectuer des signalements sur les conduites contraires au code.

Présentation des Fiches AFA

Recommandation n° 2 - Code de conduite anticorruption

Caractéristiques du Code de conduite

Rédaction :

- Il doit être formalisé par écrit.
- Il est rédigé de la façon la plus claire précise
- Il peut comporter une contextualisation de l'environnement de la collectivité
- Il est mis à jour en particulier lors des MAJ de la cartographie des risques.
- Il comporte une mention de sa date d'effet, afin de tenir compte des évolutions de l'organisation de la collectivité.

Champ d'application :

- Il est applicable à l'ensemble des agents de la collectivité.
- Il est applicable partout où la collectivité et ses agents exercent une activité.

Diffusion :

- Il est lancé par l'instance dirigeante.
- Il est diffusé à l'ensemble des agents (remis directement ou rendu accessible).
- Il est diffusé aux tiers avec lesquels la collectivité travaille.
- Il est intégré au règlement intérieur s'il existe.

Présentation des Fiches AFA

Recommandation n° 3 - Construire un dispositif d'alerte interne

Cette recommandation vise à la mise en œuvre de la remontée des alertes éthique en assurant la protection des lanceurs d'alerte en conformité avec les dispositions des articles 6 à 16 de la loi Sapin II du 9 décembre 2016

« Le dispositif d'alerte interne est la procédure mise en œuvre par les organisations afin de permettre à leurs employés, de porter à la connaissance d'un référent anticorruption, un comportement ou une situation potentiellement contraire au code de conduite, d'y mettre fin et de les sanctionner le cas échéant.

Le dispositif d'alerte interne fait partie d'un dispositif complet de prévention et de détection de la corruption. »

Extrait de la recommandation AFA n° 3

Présentation des Fiches AFA

Recommandation n° 3 - Construire un dispositif d'alerte interne

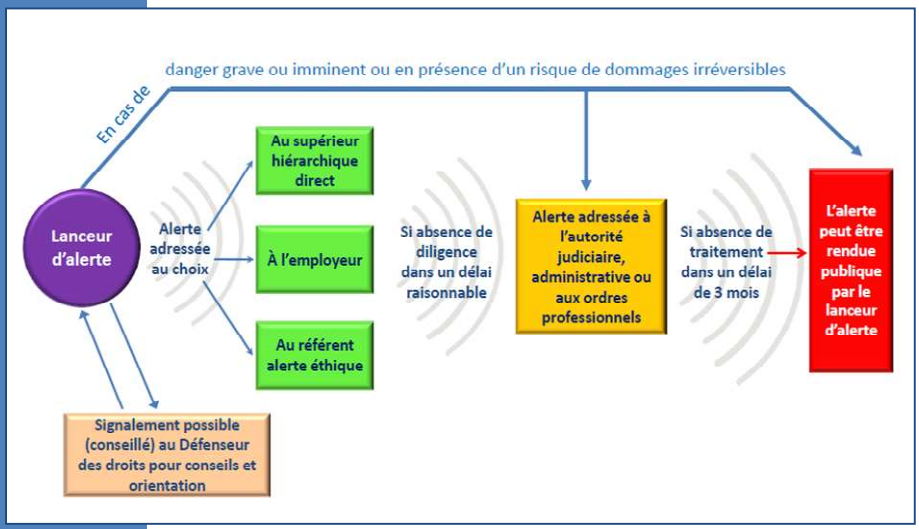


Schéma d'organisation proposé pour l'organisation du lancement d'alerte

Atelier thématique :

Atelier AFA :

"Quelle cartographie des risques de corruption ?
Quels outils de prévention et détection ?"

Animateurs :

- **Olivier WATEL**
  Chargé de mission Management des Risques
  Conseil Départemental Pas de Calais

- **Marie-Laure FERNANDEZ-VEGA**
  Contrôleur de Gestion
  CNFPT

QUESTION 1

Vous devez conseiller une collectivité (qui n'a pas forcément de connaissance pointue sur le sujet ni d'ingénierie à disposition) pour identifier et évaluer les risques de corruption.

Modalités pratiques : *Quelle méthodologie d'élaboration ? Quelles étapes de mise en œuvre ? Quelles activités sont-elles concernées ? Quelles typologies de risques ? Faites-vous une cartographie dédiée ou sont-ils intégrés dans des cartographies métiers/services ? Comment et qui fait la mise à jour ? Qui met en œuvre les plans d'action ? Qui en assure le suivi ?*

Questions à se poser – Points de vigilance

Facteurs de réussite

PROPOSITIONS :

Méthodologie :

1- Sensibilisation des agents et gouvernance
2- Définition et périmètre
3- Mode opératoire
   - Analyser les zones les plus exposées :
     - Organisation : personnes seules en charge d'un processus de A à Z. Délégations.
     - Rotation des personnes/turn-over sur leur périmètre de responsabilité en particulier sur les activités à risque. Analyse de l'ancienneté dans les fonctions en lien avec les RH. Limites : domaines, activités d'expertise. Introduire une séparation de tâches dans le processus. Contrôle de 1er et 2ème niveau
     - Identification de scenarii de corruption (catalogue)
   - Hiérarchisation (échelle) des risques. Impact (juridique, réputation, financier). Brut/probabilité
4- Cartographie des risques nets
5- Validation management
6- Pour les risques prioritaires : Traitement/actions – Suivi des actions
   Actions à mettre en place vis-à-vis des tiers : prestataires/entreprises. Réputation du tiers / Choix de prestataires : Conflit d'intérêt
7- Description du qui fait quoi
8- Actualisation

Facteurs de réussite :

- ✓ Sensibilisation : lister les cas possibles et les risques
- ✓ Formation

Pour ces deux points, c'est le rôle du déontologue mais aussi des fonctions de contrôle : contrôleurs de gestion et auditeurs internes.

- ✓ Charte : exemples concrets : « je m'engage à signaler les conflits d'intérêts… ».
  Charte de la commande publique : découpage des étapes. Analyse des risques et des comportements à chaque étape.
- ✓ Gestion du risque vis-à-vis des tiers : intégration d'exigences dans les CCTP ; engagement/signature d'une charte ; déclaration d'intérêt : exemple AMO/Candidats

QUESTION 2

Vous devez identifier des actions de maîtrise des risques de corruption.
Modalités pratiques : *Quelles actions pour lutter contre la corruption ? Quels dispositifs/outils de détection? Quels dispositifs/outils de prévention ? Quelle complexité de mise en œuvre ? Quel coût de mise en œuvre ?*
Questions à se poser – Points de vigilance
Exemples de mise en œuvre

PROPOSITIONS :

- **Informer communiquer auprès des agents et des élus:**
  - <u>Action de prévention</u> :
    - ✓ Sensibilisation et présentation : qu'est-ce que la corruption ? Définitions à clarifier. Qui est concerné ? Où se situe le risque ? Sensibilisation (actualisée) des agents, des élus y compris des auditeurs
    - ✓ Exemplarité des élus « porteurs de la démarche » : adhésion. Incarnation au niveau du top management
    - ✓ Désacraliser le risque : pédagogie, expliquer et rassurer. Fixer des définitions et de limites. Comprendre les conséquences
    - ✓ Fiches RH (au moment des Evaluations) pour présentation et sensibilisation des agents
    - ✓ Insertion d'un paragraphe engageant le signataire qu'il n'est pas en situation de conflit d'intérêt
      - agents par exemple : rapport instruction/RAO
      - élus par exemple : PV de CAO
    - ✓ Formation des agents et des élus et Formation (1/2 journée) de tous les agents en lien avec les fonds européens/les marchés publics/les subventions
    - ✓ Module formation en ligne CNFPT / FUN MOOC

<u>- Cartographier</u> : i
- ✓ identifier les secteurs et activités les plus sensibles (ex : fonction achat). Une fois les priorités identifiées : Pilotage à définir dans chaque organisation (déontologue, risk manager, audit interne…). La cartographie doit couvrir l'ensemble des services.
  Méthodologie de cartographie : Rôle de l'audit interne : Identifier, évaluer, prioriser, actions stratégie de risques. Décomposition des processus, analyse des outils.

- <u>Actions de détection</u> :
- ✓ Rôle de la 3ème ligne de défense : auditeurs internes
- ✓ Rôle du management : contrôle, traçabilité, séparation des fonctions, RH (turn over, dossier RH)
- ✓ En cas de suspicion : lanceur d'alerte, rôle de l'inspection, enquête administrative
- ✓ Concevoir les canaux de lancement d'alerte : qui reçoit les alertes ? qui décide de la suite à donner ? Exécutif ? Qui propose la suite à donner ? Lanceurs d'alerte : Traitement des alertes(mails génériques, autres) par 2 personnes au moins
- ✓ Analyse croisée à partir de requêtes sur outils de gestion
- ✓ Rôle du référent déontologue

- <u>Contrôles périodiques</u>:
- ✓ Réalisés par l'audit interne.
- ✓ Fréquence tous les 2 à 3 ans
- ✓ Intégration du risque dans les audits : plan d'audit, programmes de travail

Atelier thématique :

Atelier COSO N°5 :

"INFORMATION, COMMUNICATION ET REPORTING : comment utiliser les nouvelles technologies pour rendre compte des risques et communiquer ?"

Animateurs :

- **Jessy PETITPAS**
  Chef de Projet Audit, Appui Contrôle Interne et Evaluation
  Conseil Départemental Cher

- **Michel REVERDY**
  Directeur de l'Audit Interne
  Ville et Eurométropole de Strasbourg

Conférence des Inspecteurs et des Auditeurs Territoriaux (CIAT)

Echange d'expérience
Atelier COSO n° 5

« INFORMATION, COMMUNICATION ET REPORTING »
comment utiliser les nouvelles technologies pour rendre compte des risques et communiquer?

Animateurs de l'atelier :
Jessy PETITPAS, Chef de Projet Audit, Appui Contrôle Interne et Evaluation – CD18
Michel REVERDY, Directeur de l'Audit Interne - Ville / Eurométropole de Strasbourg

LE COSO E.R.M.

C'EST QUOI ?

COSO
Un référentiel national à double portée

COSO = acronyme d'un groupe de personnes physiques (américaines) ayant publié **2 référentiels de portée internationale** :

- l'un portant sur le contrôle interne,
- l'autre portant sur la gestion des risques.

Par facilité, on appelle « COSO C.I. » et « COSO E.R.M. » ces deux référentiels (ERM signifiant « Enterprise Risk management »)

Le **COSO C.I. :** date de 1992 / mis à jour en 2013

Le **COSO ERM :** date de début 2004 / mis à jour en 2017

=> Cette dernière version n'est pas encore traduite ni retranscrite en français

=> **L'objectif d'ici fin 2018** :
décliner ce référentiel sous forme de « fiches » opérationnelles et pratiques pour en faciliter l'application par les Collectivités

UNE METHODOLOGIE « FACILITATRICE »

20 principes déclinés du référentiel national COSO E.R.M. « risques »

Déclinaison du référentiel COSO ERM « risques » = Un appui pratique aux collectivités

- Objectif : aider les acteurs du contrôle interne

=> donner une méthodologie aux collectivités pour appréhender les risques et mettre en place un contrôle interne efficace / opérant

=> réaliser un document pratique et lisible avec des fiches facilement déclinables et opérationnelles pour les acteurs des collectivités

- Méthode : déclinaison du cadre de référence COSO ERM

=> 5 composantes : 2 « support » / 3 « opérationnelles »

=> 20 principes à décliner en **20 fiches pratiques :**

. de la stratégie - gouvernance, au pilotage, en passant par la « COM »
. pour un management des risques adapté à toutes les organisations

20 fiches « pratico-pratiques »

5 composantes du COSO ERM s'appuient sur 20 principes déclinés en 20 fiches opérationnelles pour les collectivités

. **Composante 1 : gouvernance / culture (5 fiches)**
=> ce qui encadre le risque

. **Composante 2 : Stratégie / Définition des objectifs (4 fiches)**
=> comment je prends en compte les risques dès le choix politique publique

. **Composante 3 : Performance** (5 fiches)
=> comment j'évalue les risques susceptibles de m'empêcher d'atteindre objectifs

. **Composante 4 : Revue – Amendement** (3 fiches)
=> comment je mets à jour ma vision sur les risques

. **Composante 5 : Information / Com / Reporting (3 fiches)**
=> comment j'obtiens la bonne information sur l'analyse des risques
=> comment je restitue l'info auprès de mon organisation et j'en tire profit

2ème composante support « COSO N° 5 » :

INFO / COM / REPORTING

une « check list » sur 3 PRINCIPES

3 FICHES PRATIQUES

5ème composante du COSO « information – communication – reporting »

. FICHE 18 : Tirer parti des données et des technologies

=> comment capter l'information en interne et mobiliser l'ensemble des sources ?
=> avoir les outils adaptés, les données fiabilisées => analyse /gestion des risques

. FICHE 19 : Communiquer les informations liées aux risques

=> communiquer efficacement et de manière adaptée l'information sur les risques
=> repérer/animer/mettre en œuvre les méthodes de sensibilisation/communication

. FICHE 20 : Rendre compte des risques/culture/performance

=> adapter le reporting et la communication en fonction des parties prenantes
=> réaliser un reporting adapté et ciblé :
. identifier les informations utiles à communiquer sur les risques
. s'assurer d'une opérationnalité pour les décideurs
. Veiller à une info partagée / comprise / effective

Atelier pratique en « WORK CAFE »

ECHANGES et RETOURS D'EXPERIENCE

- COSO composante 5 -

Atelier pratique « interactif » sur la 5ème composante du COSO « information – communication – reporting »

. **Modalités de mise en œuvre :**

=> modalités pratiques rencontrées dans vos collectivités / entités respectives
=> points d'attention sur lesquels vous souhaiteriez insister

. **« Ecueils » à éviter:**

=> zones d'attention ou de vigilance particulières
=> risques / freins principalement rencontrés ou pratiques à éviter

. **Exemples concrets ET « bonnes pratiques » :**

=> **initiatives** réalisées / **outils** utilisés / démarches initiées dans vos entités
=> **astuces** pour débuter la mise en œuvre OU pour aller plus loin

Rotation : 5 à 7 min sur chaque THEME => 5 personnes par table !

Merci de votre participation active, utile pour les fiches !

Animateurs - atelier COSO 5 « Information/communication/reporting »

. Jessy PETITPAS, chargée de projets
Cellule « audit-appui au contrôle interne / évaluation » au Conseil Départemental du CHER
=> Coordonnées Tel : 02.48.25.24.79 / Portable : 06.89.07.42.09 / Mail : jessy.petitpas@departement18.fr

. **Michel REVERDY, directeur de l'Audit Interne** - Ville et Eurométropole de Strasbourg
=> Coordonnées Tel 03 68 98 67 40 / Portable : 06 78 62 11 44 / Mail : Michel.REVERDY@strasbourg.eu

Atelier thématique :

Atelier sur les fondamentaux de l'Audit Interne :

"Méthodologie de réalisation d'une matrice des risques à l'appui d'une mission d'audit"

Animateurs :

- **Philippe BOISARD**
  Auditeur Interne
  Conseil Départemental Haute-Garonne

- **Myriam DEHMEJ**
  Chargée de Mission Prévention des Risques des Fonds Européens
  Conseil Régional Ile de France

Atelier : Méthodologie de réalisation d'une matrice des risques à l'appui d'une mission d'audit

Animateurs:
Myriam DEHMEJ, Chargée de Mission Prévention des Risques des Fonds Européens - Conseil Régional Ile de France
Philippe BOISARD, Auditeur Interne - Conseil Départemental Haute-Garonne

IX^{ème} Conférence des Inspecteurs et Auditeurs Territoriaux _2018

Le Risque

Un risque est la possibilité que se produise un évènement qui aura un impact sur l'atteinte des objectifs

Le risque est inhérent à toute activité
Il peut être vu comme une opportunité

Le Risque

L'appréciation du risque

Elle peut être biaisée par

- Une information limitée
- Une imagination limitée
- L'habitude du danger
- Le poids excessif accordé aux expériences passées
- Une confiance ou un pessimisme excessif
- Un conflit d'intérêt …

Le Risque

Le risque doit être évalué avec un pessimisme raisonnable

Au regard de l'état actuel de l'organisation
et non après d'hypothétiques actions

Le doute et la remise en cause sont de rigueur

Les incidents survenus peuvent donner des indications utiles

Le Risque

Il se mesure en termes d'impact et de probabilité

- **L'impact mesure la gravité des conséquences**

Il peut être financier, juridique, social, …

- **La probabilité évalue la possible réalisation du risque**

Elle est quantitative (ex: 0 à 100 %) ou qualitative (forte, rare, …)

Mesurés selon des cotations partagées

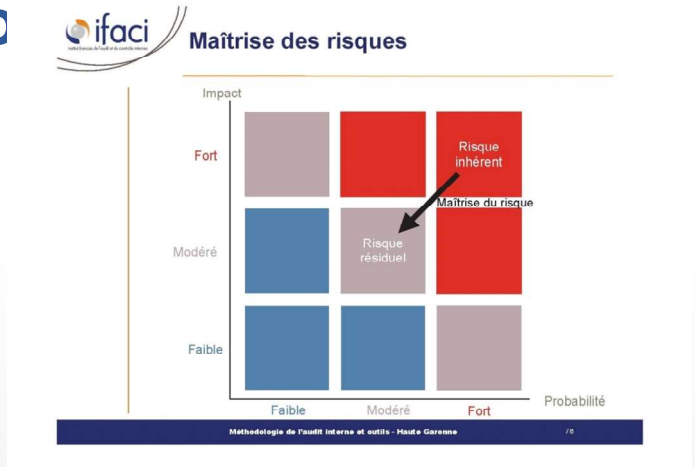
Le Risque

Risque brut, Contrôle et Risque net

- **Le risque brut** est la situation la pire suite à la survenue d'un évènement contrariant la réalisation des objectifs
- **Les mesures de contrôle**, qui permettent la maitrise des risques bruts, déterminent **le risque net**

Le Risque

La représentation carto



Phases majeurs du projet de mise en œuvre d'une gestion des risques

1 **Gestion :** Piloter le projet de mise en œuvre en assurant qu'il atteigne ses objectifs en temps, en coût et en qualité

Lancement	Pilotage	Clôture
• Définition de la structure de gouvernance à mettre en place • Définitions des rôles et responsabilité, fréquence de rencontre • Plan de projet qui détaille toutes les activités	• Analyse documentaire • Tenue des ateliers d'inventaire et de maturités des processus • Définition du modèle d'évaluation des risques (échelle et appétence) • Tenue des ateliers des risques et contrôles	• Validation de la cartographie des risques

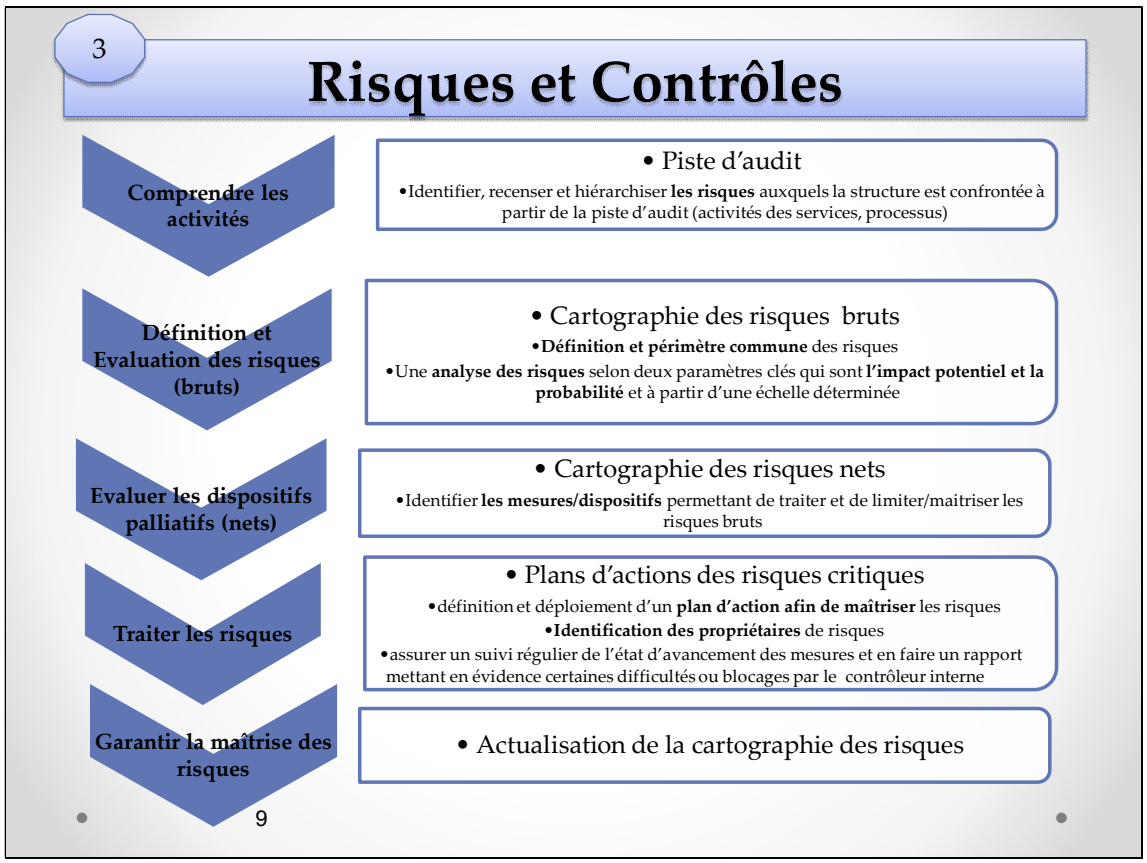
2 **Processus**

Inventaire	Maturité
• Réaliser un inventaire complet des processus existants et manquants par Dir.	• Evaluer la maturité de la Dir. quant à la maitrise de ces processus

3 **Risques et Contrôles**

Identification	Evaluation	Contrôle
• Identifier les risques des processus par Dir.	• Evaluer en termes d'impact et de probabilité ces actions pour déterminer les priorités d'action.	• Définir le plan d'action pour l'amélioration et les suivi des activités de contrôle interne.

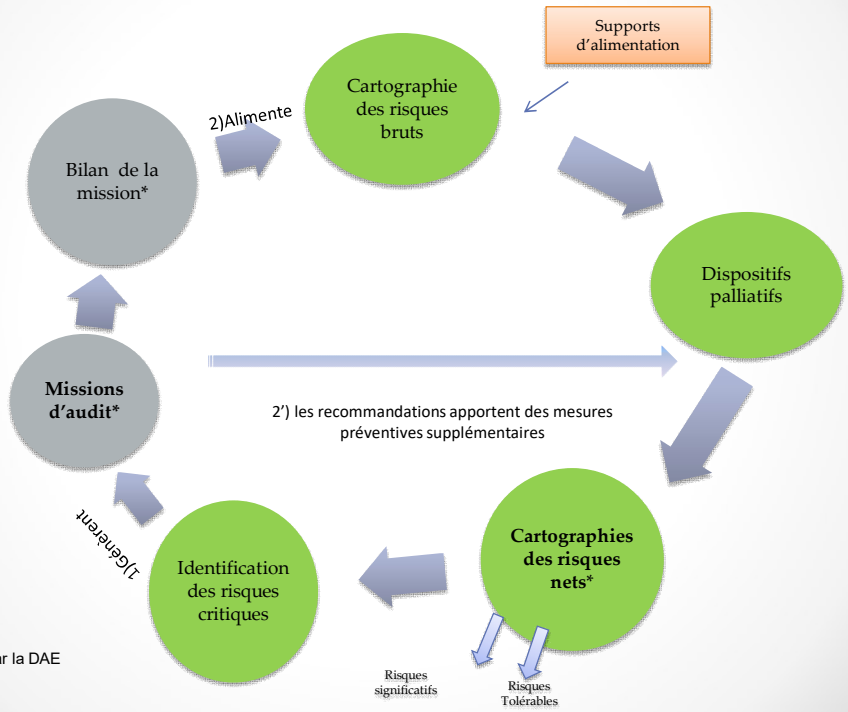
4 **Communication :** Assurer une information claire et précise sur les bénéfices récoltés par la structure via le projet



Support d'alimentation de la cartographie des risques

Phases	Sources d'informations
Inventaire complet des processus existants et manquants	• Guide des procédures • Document descriptif du système de gestion • Atelier de travail avec les responsables des Dir.
Identification des risques	• Rapport d'audit et de contrôle interne • Contrôle de service fait • Visite sur place • Entretien d'identification des risques auprès des Dir. sur la base d'un questionnaire • Notes stratégiques • Inventaire des processus et des dysfonctionnements s'y afférents • Changement dans le fonctionnement et l'organisation d'une Dir. • Evolution des textes réglementaires
Evaluation des risques	• Création d'une échelle en impact et en probabilité du taux de criticité des incidents constatés • Suivi des plans d'action • Suivi des indicateurs d'objectifs

Articulation entre la cartographie des risques et les missions d'audit : Auto-alimentation



*Etape de validation par la DAE
•DAE
•DAECG

11

Les premières difficultés rencontrées

- Le retard pris dans la finalisation des missions d'audits.
- La difficulté d'identifier des indicateurs d'objectifs pertinents, mesurables et fiables
- Le glissement opéré entre les risques significatifs et les risques critiques (*piste d'amélioration: apporter des actions sur les risques les plus significatifs)*
- Le traitement manuel de plusieurs données différentes à consolider peut entrainer des erreurs *(piste d'amélioration: nécessité de disposer d'outils).*
- Difficulté d'interpréter la notion de risque *(piste d'amélioration : participer à l'élaboration du plan d'action en lien avec la direction responsable de sa mise en œuvre afin de lever toute ambiguïté sur la définition et sur l'interprétation du risque)* .
- Difficulté d'identifier la part de risque des directions en cas de co/propriétaires de risques, *(Piste d'amélioration: Intégrer l'ensemble des parties prenantes tels que la direction des affaires juridiques, commande publique à la démarche d'actualisation de la cartographie des risques et du plan d'action).*

12

Atelier thématique :

Atelier sur les fondamentaux de l'Audit Interne :

"Quel suivi efficace des recommandations ?"

Animateurs :

- **Bruno BORODINE**
  Directeur de l'Audit
  Conseil Régional Bretagne

- **Stéphane LABONNE**
  Mission d'Inspection Générale
  Conseil Régional des Pays de la Loire

Atelier sur les fondamentaux de l'audit interne

Quel suivi efficace des recommandations ?

Intervenants :

- Bruno BORODINE - Direction de l'audit - Région de Bretagne
- Stéphane LABONNE - Inspection générale - Région des Pays de la Loire

IXème Conférence des inspecteurs et auditeurs territoriaux

Toulouse - 12 octobre 2018

Fondements et enjeux

Fondements

Pour les audits internes

Norme 2500 du Cadre de référence international des pratiques professionnelles (CRIPP) relative à la surveillance des actions de progrès

Le responsable de l'audit interne doit mettre en place et tenir à jour un système permettant de surveiller les suites données aux résultats communiqués au management.

Pour les observations de la Chambre régionale des comptes

Article L243-7 du Code des juridictions financières

Dans un délai d'un an à compter de la présentation du rapport d'observations définitives à l'assemblée délibérante, l'exécutif de la collectivité territoriale ou le président de l'établissement public de coopération intercommunale à fiscalité propre présente, dans un rapport devant cette même assemblée, les actions qu'il a entreprises à la suite des observations de la chambre régionale des comptes.

Fondements et enjeux

Qu'est-ce qu'une recommandation ?

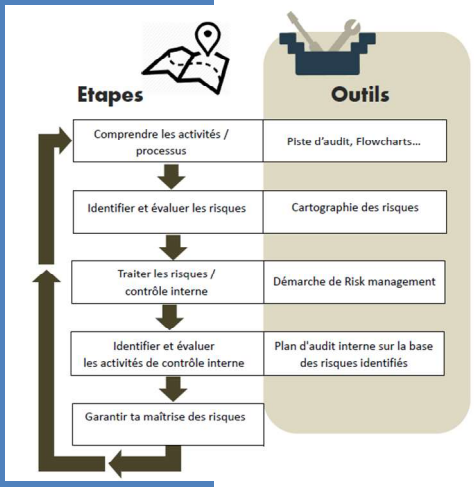
- Une recommandation procède d'un constat lié à un risque identifié
- Une recommandation peut revêtir un caractère préventif ou correctif
- Une recommandation n'est pas un plan d'action
- Une recommandation est formalisée dans le rapport d'audit

Qu'est-ce qu'un plan d'actions ?

- Un plan d'actions répond à une recommandation et constitue une mesure de maîtrise pour couvrir un risque
- Un plan d'actions est défini par le responsable du domaine ou du processus audité (selon le périmètre de l'audit)
- Tout plan d'actions est affecté d'un ou plusieurs pilote(s) nommément identifié(s), d'un calendrier et de points de vérification sous la forme de preuves et/ou d'éléments matériels permettant de vérifier la réalisation des actions prévues

Fondements et enjeux

Intégration du plan d'actions dans le dispositif de contrôle interne de la collectivité



Le suivi des recommandations est efficace s'il se retrouve dans le processus de maîtrise des risques de la collectivité (risk management).

Le plan d'actions peut ainsi être permanent et intégrer à ce titre le dispositif de contrôle interne de la collectivité.

Dans ce cadre il contribue à l'objectif de réduction des risques résiduels et concourt à la dynamique de suivi de la cartographie des risques.

Modalités de mise en œuvre

Quel reporting ?

Possibilités de reporting :

- A minima le directeur général et/ou l'équipe de direction (CODIR…)
- S'il existe, le comité d'audit
- Eventuellement un comité dédié (comité de suivi et/ou comité des risques…)
- …

+ Reporting éventuel à l'assemblée délibérante (selon une forme à déterminer)

Quand ?

Laisser passer un laps de temps entre la notification du rapport définitif et le suivi des recommandations

Regrouper l'ensemble des suivis à une échéance fixée annuellement (par exemple sur la base de deux revues par an)

Pour traiter les cas de non-exécution sans justification recevable, prévoir une alerte auprès des instances de reporting

→ S'agissant des observations de la Chambre régionale des comptes, voir l'article L 243-7 du Code des juridictions financières

Comment ?

Toutes les recommandations doivent-elles être suivies ? Prévoir éventuellement une classification selon la criticité du risque (par exemple de une à trois étoiles)

Renseigner une base de suivi des recommandations en utilisant un nombre prédéterminé de statuts (réalisé, en cours, abandon / changement de contexte)

Etablir une synthèse quantitative et qualitative par audit

Consolider ces éléments dans une synthèse couvrant une période de 6 à 12 mois

+ Possibilité de réalisation d'un **audit de suivi** pour vérifier l'effectivité des suites données

Pour aller plus loin…

Collecter et vérifier les preuves matérielles associées à chaque action réalisée, cette preuve étant susceptible d'être rejetée s'il apparaît qu'elle ne couvre pas la recommandation

Réaliser des visites sur place afin de s'assurer de la mise en application effective des mesures correctrices prévues

Mettre en place des indicateurs pour mesurer la performance de l'audit interne et la pertinence des recommandations formulées (par exemple le % de réalisation du plan d'action à l'échéance fixée)

Modalités de mise en œuvre

Des supports adaptés à chaque étape…

Tableau de suivi des recommandations

Fiche de synthèse pour le suivi des recommandations de l'audit (document clôturé à l'issue du plan d'action et conservé dans le dossier d'audit)

Fiche de synthèse pour le suivi des recommandations à l'échelle de la collectivité sur une période fixée (document utilisé notamment pour le pilotage du risk management)

Formulation des recommandations dans les rapports d'audit → **Suivi des recommandations par audit** → **Suivi global des recommandations**

Atelier thématique :

Atelier "décalé" :

"L'Audit Interne : règles de survie dans la vraie vie"

Animateurs :

- **Alain COUTURIER**
  Directeur des Contrôles, des Audits et de l'Expertise
  Conseil Régional Occitanie

- **Hélène MATHIEU**
  Directrice Générale de l'Inspection Générale
  Ville de Paris

Cette séquence avait été inscrite dans le programme en tant qu' « atelier décalé » et, comme son titre pouvait le laisser présager, les échanges ont été denses et la participation très active.
Le nombre des participants qui ont effectivement poussé la porte de cet atelier a semblé supérieur au nombre d'inscriptions préalables, mais peut-être est-ce l'annonce du tirage au sort des sujets dans un véritable béret pyrénéen qui a attisé leur curiosité.
L'atelier avait été construit autour d'une quinzaine de sujets qu'un binôme d'animateurs (Hélène Mathieu, Directrice de l'Inspection Générale de la Ville de Paris et Alain Couturier Directeur des Contrôles, des Audits et de l'Expertise en Région Occitanie) avait préalablement rédigés, sur la base de leur expérience partagée, et imprimés sur des billets présentés à l'assistance pour tirage au sort.
Tirage d'un sujet, lecture à haute voix (parfois avec étonnement) du contenu du billet et démarrage des échanges autour du thème ainsi exposé. Est-ce une situation que vous avez déjà rencontrée, si oui comment l'avez-vous traitée ? Sinon, que pensez-vous qu'il conviendrait de faire dans pareil cas ?

Les sujets soulevés ont eu de nombreux échos auprès des participants, certains ayant pu s'exprimer sur des expériences personnelles très intéressantes à partager, parfois même empreintes d'émotion quand les questions abordées touchaient des moments forts vécus par certains(es) auditeurs(trices). Échanges intenses et fructueux.
Les animateurs complétaient, précisaient, à partir de leur expérience, les conclusions à tirer ou les recommandations pour le cas où un participant serait amené à croiser sur sa route professionnelle une situation du même type.

Figure ci-dessous la liste des sujets. Tous n'ont pas été examinés compte tenu du temps contraint de l'atelier. Mais qu'à cela ne tienne, un auditeur prévenu en valant deux, voici de quoi se préparer grâce aux antisèches, conseils et règles qui figurent en face de chacune des situations évoquées!
Les intrépides animateurs de cet atelier décalé ne reculant devant aucun danger dévoilent ici l'intégralité des sujets et des réponses préalablement préparées dont on retiendra qu'elles ont été, en séance, mille et une fois enrichies par les propos des participants.
En conclusion ce type d'atelier d'échanges de pratiques professionnelles concrètes est à refaire lors de la prochaine CIAT. Nous comptons sur vous, l'année prochaine, pour enrichir les pratiques ainsi capitalisées.

Situation	Conseils et règles applicables
1. Lors de votre deuxième réunion du Comité d'Audit, le DGS vous fait faux bond à la dernière minute et n'assiste pas à la réunion	**1.** Charte d'audit : prévoir le fonctionnement du Comité, en cas d'absence du pilote de cette instance **2.** Support d'animation : il est complet, détaillé (texte/graphique) et structuré (rappel, information, proposition de décision)
2. Lors de la réunion de lancement d'un audit portant sur un organisme subventionné par la collectivité, le DG, le Maire ou le président du conseil départemental ou son représentant qui assiste normalement à la réunion vient accompagné du Président de la structure à qui il a « vendu » le principe d'une étude et non pas d'un audit	**1.** Rappel du jeu d'acteurs, de la séparation des fonctions, du déroulé de la procédure, de la place (dans un second temps) du contradictoire dans la démarche. **2.** Ramener les échanges à des éléments factuels dont l'analyse va être confiée aux auditeurs **3.** Rappeler les principes déontologiques fondamentaux auxquels sont soumis les auditeurs : indépendance, intégrité, objectivité, confidentialité, compétence, professionnalisme

Situation	Conseils et règles applicables
3. Lors de la restitution d'un audit portant sur un organisme extérieur financé par la collectivité, le cabinet d'audit fait apparaitre un pb de suivi de la part de la direction opérationnelle en charge de cet organisme et la chargée de mission concernée part à la faute.	**1.** Rappel du rôle de l'audit dans les processus d'amélioration continue **2.** Inscrire les recommandations dans le calendrier d'un plan d'action **3.** Mettre l'accent sur ce qui va mieux fonctionner
4. Lors d'une restitution d'audit ou de la remise du rapport définitif, le DG ou le Maire ou Président du CD réagit mal, expliquant que le rapport ne répond pas à la commande initiale	**1.** Formaliser au préalable la commande (seuls les écrits restent) **2.** Des travaux d'approfondissement d'un point particulier sont toujours possibles **3.** Rappeler le positionnement des acteurs (3ème ligne de maîtrise), et la logique de sécurisation de l'action publique, l'intérêt du long terme p/r aux contraintes immédiates du court terme **4.** Rappel de la possibilité de conserver un caractère confidentiel au rapport d'audit (obligations de confidentialité des auditeurs) en mettant l'accent sur l'intérêt du plan d'actions
5. Un Président d'organisme audité, un ou des élus tentent d'instrumentaliser un rapport d'audit	**1.** Le Comité d'Audit et la direction de l'audit restent les maîtres du temps. **2.** Le rapport ne contient pas de données d'un tiers de comparaison
6. Vous recevez appels téléphoniques mails ou invitations à déjeuner, autant de pressions pour vous faire abandonner l'audit	**1.** Rappel des obligations d'indépendance, courtoisie et politesse **2.** Report après la phase d'audit
7. Vous êtes gravement mis en cause et « lâché » par les élus ou le DG sur l'absence de déontologie d'un rapport suite aux interventions d'un groupe de pression (enseignants de conservatoires, familles d'accueil de l'aide sociale à l'enfance, travailleurs sociaux, milieu sportif…	**1.** Rappel des normes d'audit, du professionnalisme des auditeurs et du code de déontologie **2.** Dialogue, concertation, et phase contradictoire ne signifient pas accord et consensus. Les faits ne doivent pas pouvoir être contredits et l'auditeur doit s'appuyer sur ces éléments. Les interprétations des faits sont par nature subjectives.
8. Un rapport vous semble insuffisamment étayé	**1.** Différer la phase de restitution. **2.** Si impossible, caractériser l'acquis et proposer une phase d'approfondissement dans un calendrier maîtrisé pour les points à développer
9. Un rapport vous semble rédigé à charge	**1.** Bloquer le rapport, s'entretenir avec les auditeurs pour confirmer / infirmer cette perception. **2.** Demander si nécessaire un approfondissement

Situation	Conseils et règles applicables
10. Vous concluez suite à une enquête à la nécessité de rédiger un article 40 au procureur de la République mais le DG ou l'élu est contre, le service des affaires juridiques peu enclin, car ils craignent des fuites et une exploitation par la presse aux retombées négatives	**1.** Rappeler les termes de la réglementation article 40 (obligations) **2.** Mettre l'accent sur la sécurisation de l'action de la collectivité **3.** Souligner la quasi-impossibilité de garantir une étanchéité absolue (poids des réseaux sociaux dans la société actuelle), la tentative d'omerta pouvant se révéler bien pire que le mal
11. Un (ou plusieurs) auditeur refuse la mission qui figure au programme d'audit et que vous souhaitez lui confier car il juge le sujet trop explosif ou s'estime trop exposé	**1.** Recourir à une prestation extérieure (si existence d'un marché en ce sens) **2.** Apparaitre comme le pilote de la mission d'audit pour protéger les auditeurs, en leur confiant des tâches plus techniques et des traitements en backoffice
12. Un ou plusieurs services ou structures audités mettent 4 à 6 mois pour répondre en phase contradictoire et vous endossez malgré vous le retard pris pour la remise du définitif	**1.** Oui mais là il aurait fallu réagir bien plus tôt… systématiser l'instauration d'un délai de réponse, voire une clause du type « en l'absence de réponse/observation écrite de votre part au …, le contenu de ce rapport sera considéré comme approuvé » **2.** Tracer les échanges sur les délais à la manière d'une direction de projet
13. Vous devez annoncer aux auditeurs chargés d'une mission qui a démarré qu'elle doit être abandonnée car l'administration a démarré entre temps une réforme de structure et la hiérarchie de veut pas la « gêner »	**1.** S'appuyer sur le rôle du Comité d'Audit, sa responsabilité dans la programmation des audits / gestion des modifications. **2.** Mettre l'accent sur les enjeux pour la collectivité et sa stratégie, au regard des différents calendriers (temps politique, temps administratif, temps technique, …)
14. Vous constatez qu'aucun plan d'action n'a été mis en œuvre suite aux recommandations d'un rapport, que faites-vous ?	**1.** S'appuyer sur le plan initialement rédigé, rechercher les causes (factuelles), s'intéresser à la compréhension des différents enjeux, établir un nouveau calendrier, resserrer les conditions de suivi