REPUBLIQUE DEMOCRATIQUE DU CONGO

MISE EN OEUVRE DE L'AUDIT ET DU CONTRÔLE INTERNES
AU SEIN DES ADMINISTRATIONS PUBLIQUES

GUIDE METHODOLOGIQUE DE L'APPROCHE DE MANAGEMENT, DE CONTROLE INTERNE ET D'AUDIT PAR LES RISQUES

MINISTERE DES FINANCES

Comité d'Organisation
de la Réforme des
Finances Publiques

Equipe rédactionelle

Ce guide a été élaboré par Monsieur Souleymane SERE, sous la coordinnation de Monsieur Victor Batubenga Mbayi, Inspecteur Général des Finances - Chef de service et de Monsieur Godefroid Misenga, Coordonnateur du Comité d'Orientation de la Réforme des Finances Publiques. Il a bénéficié de la participation de Monsieur Camille José Mabele, Inspecteur Général des Finances - Chef de service Adjoint et de Monsieur Etienne Mafweni, Assistant Technique au COREF.

AVEC LE FINANCEMENT DU PROJET DE RENFORCEMENT DE LA REDEVABILITE
ET DE LA GESTION DES FINANCES PUBLIQUES
« PROFIT-CONGO »

ROYAUME DE BELGIQUE

LA BANQUE MONDIALE

UKaid
from the British people

AVANT-PROPOS

Le Gouvernement de la République Démocratique du Congo a mis en place le Projet de Renforcement de la Redevabilité et de la Gestion des Finances Publiques (PROFIT-CONGO) dont le Comité d'Orientation de la Réforme des Finances Publiques (COREF) assure la gestion fiduciaire en collaboration avec les structures bénéficiaires, celles-ci assurant la mise en œuvre au opérationnelle des actions et mesures des réformes inscrites dans le plan d'actions prioritaires de la réforme des finances publiques.

Ce projet est financé par un fond multi-bailleurs qui est alimenté par un Don de 30,2 millions de dollars américains obtenu de la Banque Mondiale, du Département du Développement International du Royaume Uni (DFID) et du Royaume de Belgique au titre de contribution initiale.

Au nombre des bénéficiaires de ce projet on compte : les services publics à caractère financier des Ministères du Plan, du Budget et des Finances ; l'Inspection Générale des Finances ; la Cour des Comptes, les Commissions Economiques et Financières du Parlement ; les Organisations de la Société Civile et les Gouvernements provinciaux du Nord-Kivu, du Kasaï Oriental, de l'Equateur et de la ville de Kinshasa.

Initié dans l'objectif d'accroître la transparence et la responsabilité dans la gestion et l'emploi des fonds publics à l'échelon de l'administration centrale et des certaines entités infranationales, le projet PROFIT-Congo vise, dans sa sous-composante 1.1 : *Appui à la déconcentration de l'Ordonnancement auprès des ministères sectoriels*, à contribuer à la mise en œuvre effective des dispositions de la loi n°11/011 du 13 juillet 2011 consistant à ramener la gestion des moyens, notamment financiers, auprès des décideurs du secteur dans le but de leur permettre d'être véritablement responsables de la réalisation de leurs objectifs. Ce nouveau cadre de gestion budgétaire, caractérisé par la redéfinition du rôle des principaux acteurs de la gestion des finances publiques de l'État, nécessite une restructuration des administrations publiques.

C'est dans cette optique que le Gouvernement vient de procéder à la création des Directions Administratives et Financières (DAF) au sein des administrations publiques en vue de renforcer la fonction de gestion budgétaire au sein des ministères sectoriels.

Parallèlement à cette démarche, la réforme de la déconcentration de l'Ordonnancement devra être également accompagnée des mesures de renforcement des capacités des structures de contrôle interne au sein des ministères sectoriels afin de minimiser les risques de dérapage liés à une plus grande autonomie. En effet, il ne serait pas raisonnable de donner cette marge de manœuvre supplémentaire aux ordonnateurs s'ils n'étaient guidés dans leurs choix par un dispositif leur permettant d'identifier les implications de leurs décisions et les faiblesses du contrôle interne.

Ce renforcement est d'autant plus nécessaire qu'au stade actuel, les structures de contrôle interne souffrent d'un manque de moyens de financement des activités et sont constituées, dans la majorité, d'un personnel insuffisamment formé aux méthodes modernes de gestion et travaillant, de manière quasi généralisée, sans procédures écrites à jour.

C'est pour cette raison que le Gouvernement de la République Démocratique du Congo a, à travers le **Projet de Renforcement de la Redevabilité et de la Gestion des Finances Publiques** recouru au service d'un consultant international aux fins d'améliorer l'efficacité et l'efficience de quelques structures de contrôle interne à savoir de l'Inspection Générale des Finances et des inspections techniques des ministères de l'Agriculture, du Développement rural, de l'Éducation, de l'Infrastructures et de la Santé par l'introduction de l'approche d'audit basé sur les risques.

L'assistance technique du consultant a porté sur l'étude des modalités d'instauration au sein des administrations publiques de l'approche d'audit basé sur les risques (ABR) ; méthodologie de contrôle visant à rationnaliser l'exercice du contrôle surtout dans un contexte de ressources financières limitées tout en respectant les principes de la nouvelle gestion publique. Elle permet d'élaborer une cartographie des risques et de cibler avec plus d'efficacité, les domaines à risques les plus élevés.

Au finale, le but poursuivi par le Gouvernement est celui d'accroître leurs performances tout en respectant les contraintes de gestion.

Le présent document a l'avantage de fournir :

- des outils de réflexion permettant de comprendre la vision et les enjeux, les principes et les concepts, les référentiels et les méthodes, les évolutions présentes et futures, les limites, les rôles et responsabilités des différents acteurs du contrôle interne et du management des risques dans le secteur public ;

- des outils d'élaboration de la cartographie des risques, de mise en œuvre et de pilotage du dispositif de contrôle interne tels que définis par le COSO 2013 : questionnaires, matrices d'identification et d'évaluation des risques, registre des risques et plan de mitigation ;

SOMMAIRE GENERAL

Liste des principaux acronymes

ABR	:	Audit Basé sur les Risques
AG – SE	:	Assemblée Générale des Sociétés d'Etat
AI	:	Auditeur Interne
CA	:	Conseil d'Administration
CDMT	:	Cadre de Dépenses à Moyen Terme
COREF	:	Comité d'Orientation de la Réforme des Finances Publiques
DAF	:	Directions Administratives et Financières
DFID	:	Département du Développement International du Royaume Uni
DG	:	Direction Générale
DMR	:	Dispositif de maîtrise des risques
ERM	:	Enterprise Risk Management
FAR	:	Feuille d'd'audit et de recommandations
GFP	:	Gestion des Finances Publiques
GFS	:	Government Finance Statistics
GRH	:	Gestion des Ressources Humaines
IFACI	:	Institut Français de l'Audit et du Contrôle Internes
IGF	:	Inspection Générale des Finances
IIA	:	Institute of Internal Auditors
INTOSAI	:	Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques
ISO	:	International Standards Organization
IxP:	:	Impact x Probabilité
LOLF	:	Loi Organique sur les Finances Publiques
MPAFC	:	Manuel de Procédures Administratives, Financières et Comptable
NBE	:	Nomenclature Budgétaire de l'État
OCDE	:	Organisation de Coopération et de Développement Economiques
OMD	:	Objectifs du Millénaire pour le Développement
PCA		Président du Conseil d'Administration
PME	:	Petites et Moyennes Entreprises
PROFIT-Congo	:	Projet de Renforcement de la Redevabilité et de la Gestion des Finances Publiques
PTF	:	Partenaire Technique et Financier
PUIUR	:	Programme d'Urgence d'Infrastructures Urbaines
RSE	:	Responsabilité Sociale des Entreprises
SE	:	Société d'État
SYSCOA	:	Système Comptable Ouest Africain
TaRiR	:	Tableau des risques référentiel
TFfa	:	Tableau des forces et des faiblesses apparentes
TOFE	:	Tableau des opérations financières de l'État
UE	:	Union Européenne
UEMOA	:	Union Economique et Monétaire Ouest Africaine

METHODOLOGIE ET OUTILS D'ELABORATION DE LA CARTOGRAPHIE, DU PLAN DE MITIGATION ET DU PLAN D'AUDIT BASES SUR LES RISQUES	**Date :**	**Durée :**
Séquence 1 : Le Management des risques dans le secteur public : principes et implications	**Classement : Sq1**	**Rédacteur : SS**
Objectifs	♦ Comprendre les principes du management des risques et les responsabilités associées	

Déroulement

Exposés :

N° Fiches	Titres / Contenu	Stratégie d'animation
Cas	Etude de cas introductif (voir fin du document : page 117) : MANAGEMENT DES RISQUES ET RESPONSABILITE DES GOUVERNANTS	**Etude de cas : Lecture et commentaire (L'Eau à Dakar: Services publics, intérêts privés et choix stratégiques)**
1	Les définitions du risque	Illustrations et cas pratiques
2	Le Gouvernement d'entreprise dans le secteur public	Illustrations
3	Le cadre de référence relatif au management des risques du COSO2	Illustrations
4	Rôle et responsabilités dans le cadre du dispositif de management des risques	Illustrations
QCM	QCM séquence Management des risques	Travaux de groupe

FICHE N°1 Les définitions du risque

1. Quelques définitions (les mots clés de la définition de l'AI à comprendre)

1.1 Concept de Risque :

Possibilité que se produise un événement susceptible d'avoir un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité ou occurrence.

***Nota** : il n'y a de risque que par rapport à l'atteinte d'un objectif ou plus précisément par rapport à la conséquence dommageable de ce risque quant à l'atteinte d'un objectif.*

Un exemple (illustration) dans notre quotidien :

- La notion de risque est associée :
  - D'une part à celle d'***incertitude*** et ***d'évènements incertains*** : ***« il risque de pleuvoir »***
  - D'autre part à ***ce que l'on encourt*** si l'évènement se réalise : ***« je risque de me faire mouiller ou tremper »***

- Dans cet exemple **l'objectif est implicite** : ***« rester sec et net »,*** mais il aurait mieux fallu l'expliciter.

- les éléments de la définition dans notre exemple :
  - L'événement incertain = la pluie (qui peut tomber : probabilité)
  - Objectif dont la réalisation pourra âtre compromise : *rester sec et net*

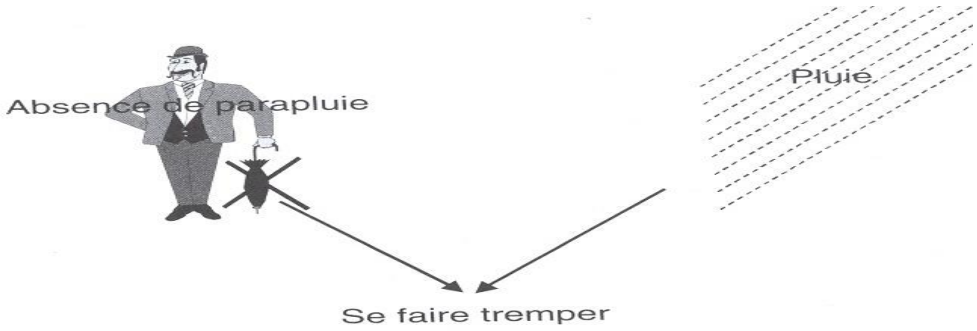
- Questions : comment gérer le risque de se faire mouiller ?
  - Ne pas sortir
  - Sortir avec un parapluie pour ne pas se faire surprendre

- Il a plu, je suis mouillé : Questions ?
  - Quelle est la circonstance (l'occasion)
  - Quelle est la cause ?
  - Quelle est la conséquence ?

- Il a plu, je suis mouillé : Réponses
  - Quel est l'évènement ou la circonstance (qui n'est plus incertain) : la pluie (l'avènement de la pluie)
  - Quelle est la cause ? c'est le fait d'être sortie sans parapluie (pluie combinée avec l'absence de parapluie) : en effet je ne suis pas tremper parce qu'il a plu **mais parce qu'à la fois il a plu et je suis sorti sans parapluie (une cause[1] : l'absence de parapluie…)**
  - Quelle est la conséquence ? **je suis trempé (je ne suis pas sec et net : donc objectif compromis = conséquence)**

[1] A y réfléchie, il s'agit d'une cause maîtrisable

Qu'est-ce qu'un risque ?

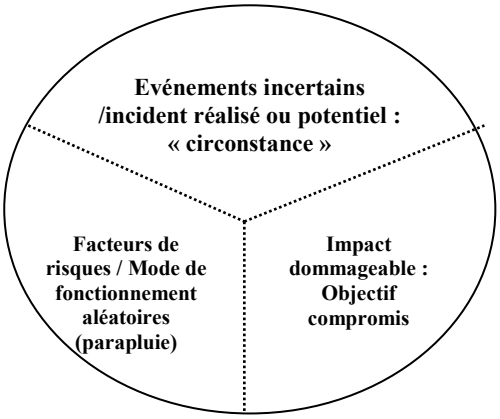


Exercices : concept de risque

L'entreprise Goama est tombée en faillite, le comptable, cousin du « PDGP » a fui avec les fonds. Questions :

- Quelle est la circonstance, l'évènement ?
- Quelle est la conséquence ?
- Quelle sont les causes possibles ?

D'**où la définition suivante du concept de risque :**	Le RISQUE est un concept désignant la possibilité que la combinaison d'un évènement incertain et d'un mode de fonctionnement aléatoire ait pour conséquence la non - atteinte d'un objectif



Maîtrise des risques = Contrôle interne

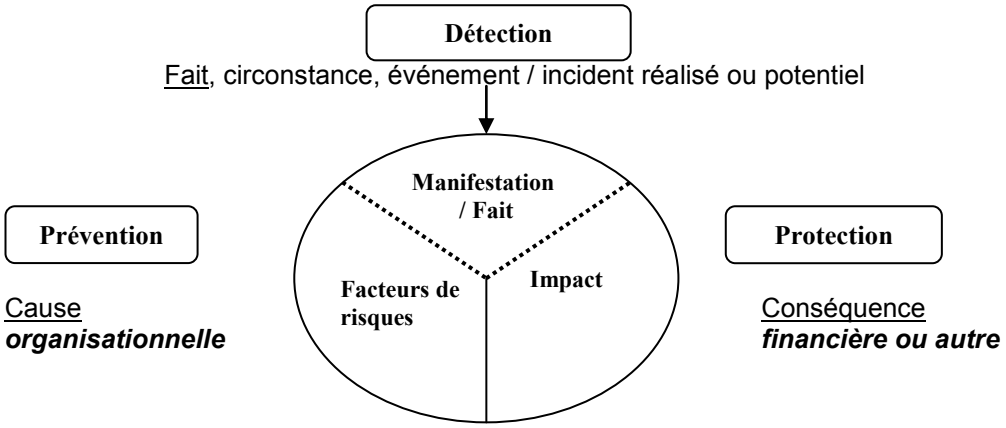
Les facteurs de risque qui, combinés à la survenance de ces événements vont ou ne vont pas entraîner de conséquences dommageables, sont tous à rechercher dans l'organisation et le fonctionnement de l'entité auditée, c'est le rôle de l'auditeur.

Par exemple, pour pallier les risques d'incendie de la salle informatique, nous allons prendre des mesures de :

1. **Prévention** pour éviter l'incendie : panneaux d'interdiction de fumer et cendriers pour écraser sa cigarette, sensibilisation / formation du personnel au risque d'incendie ;
2. **Détection** pour s'apercevoir que l'incident redouté est survenu malgré les mesures de prévention : détecteurs de fumées et de chaleur, en général au plafond ;

3. **Protection** pour limiter les dégâts occasionnés par l'incendie sprinklers et diffuseurs de gaz inertes, portes coupe-feu, assurance, coffres ignifuges…

Les facteurs de risque sont des lacunes de l'organisation qui, combinés à la survenance d'événements, vont entraîner des conséquences dommageables.



C'est ce que l'auditeur recherche car il est un « préveneur » de risques.

Cause + Circonstance = Conséquence
Et trois types de mesures pour pallier les facteurs de risques : **prévention, détection, protection**.

Nota :

- l'auditeur ne contrôle, ni ne vérifie : il **évalue et propose des améliorations**
- l'auditeur ne dénonce ni n'accuse : il arbitre « les règles du jeu » du groupe en faisant pratiquer les 3R :
    - Rechercher
    - Reconnaitre
    - Remédier **AUX FAIBLESSES DE L'ORGANISATION**

FICHE N°2 Le Gouvernement d'entreprise dans le secteur public

1. La notion de Gouvernement ou gouvernance d'entreprise : « Corporate governance »

Le gouvernement d'entreprise définit les relations entre les actionnaires, le Conseil et ses comités spécialisés et la Direction Générale. Dans ce cadre, le Conseil a un rôle de surveillance des activités de la Direction Générale dans le but d'atteindre les objectifs de l'organisation.

Le glossaire du Cadre de référence international des pratiques professionnelles de l'audit interne (les Normes) de l'IIA décrit la gouvernance comme **« le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs ».**

Le gouvernement d'entreprise touche les grands domaines (voir également Art. 435 de l'Acte uniforme sur le Droit des Sociétés Commerciales de l'OHADA) :

- La direction stratégique de l'entité : Il revient au Conseil de donner l'orientation stratégique et les lignes directrices relatives à la définition des objectifs clés de l'organisation qui doit cadrer avec les priorités des parties prenantes.
- Le Conseil doit, ensuite, surveiller les avancées vers la réalisation des buts et objectifs de l'organisation (à travers le système de reporting et les tableaux de bord).
- Après avoir cerné les besoins des principales parties prenantes, le Conseil s'attache à leur satisfaction.
- Le conseil a une responsabilité fiduciaire vis-à-vis des parties prenantes auxquelles il doit rendre compte (exigence de reporting opérationnel, financier et comptable).
- Au quotidien, la gouvernance est exercée par la direction de l'organisation, l'encadrement supérieur (propriétaire des risques) et les cadres intermédiaires à travers les activités de management des risques.
- La direction générale et le management supérieur rendent compte au Conseil à une périodicité définie (reporting).

2. La gouvernance dans le secteur public (voir normes de contrôle interne à promouvoir dans le secteur public - *Informations complémentaires sur la gestion des risques des entités* de l'INTOSAI : INTOSAI GOV 9130 ; articles 13 et 17 des Directives portant Lois des finances de l'UEMOA et de la CEMAC)

▸ Dans le secteur public, la gouvernance englobe :

- les politiques et les procédures servant à orienter les activités d'une organisation en vue de fournir l'assurance raisonnable que les objectifs sont atteints et que les activités sont menées de façon éthique et responsable.
- les moyens utilisés pour établir et atteindre les objectifs.
- Elle recouvre enfin les activités qui assurent la crédibilité du secteur public, une prestation équitable des services et l'adoption de comportements appropriés par ses représentants réduisant ainsi le risque de corruption publique.

▸ Les principes de gouvernance ci-après s'appliquent tout aussi bien aux organismes du secteur privé qu'à ceux du secteur public, bien qu'ils soient décrits dans les termes propres au secteur public :

Donner le ton qui convient. Une saine gouvernance comprend l'établissement de politiques qui orientent les actions de l'organisation.

Au sein de l'Etat, les politiques peuvent s'exprimer par la voie des grands objectifs nationaux, des plans stratégiques, des objectifs de performance, des orientations législatives, des organismes de surveillance désignés ou des comités de surveillance législative.

Les politiques de l'État ou du moins ses priorités se trouvent généralement enchâssées dans son budget, lequel a pour objet de répartir des ressources limitées entre diverses activités.

Inculquer des valeurs d'éthique et d'intégrité. Une saine gouvernance comprend des valeurs éthiques, des objectifs et des stratégies clairement articulés; le ton mobilisateur donné par la direction; et le contrôle interne.

Les politiques et les procédures doivent être alignées de manière à encourager l'adoption de comportements conformes aux valeurs d'éthique et d'intégrité de l'organisme public. Pour favoriser l'adoption de comportements conformes aux valeurs d'éthique et d'intégrité, il importe notamment d'établir des lignes claires de reddition de comptes et de veiller à leur respect pour que les personnes soient tenues responsables d'adopter les bons comportements.

Superviser les résultats. Une saine gouvernance exige une surveillance continue afin de s'assurer que les politiques sont appliquées comme prévu, que les stratégies sont réalisées et que la performance globale du secteur public répond aux attentes et aux besoins dans les limites des politiques, des lois et de la réglementation.

« Dans presque tous les ressorts territoriaux, le secteur public joue un rôle important au sein de la société, et une saine gouvernance peut y favoriser une utilisation efficiente des ressources, renforcer la reddition de comptes à l'égard de ces ressources, améliorer la gestion et la prestation des services et, par conséquent, améliorer la vie des citoyens. Une saine gouvernance est également essentielle au maintien de la confiance dans les entités publiques une condition sine qua non de la réalisation efficace des objectifs des entités publiques. »[2]

Rééditer les comptes. Comme les organismes publics agissent à titre d'« agents » qui utilisent les ressources et les pouvoirs qui leur sont confiés pour atteindre des objectifs établis, elles doivent rendre compte de l'utilisation des ressources et des résultats obtenus. Par conséquent, une saine gouvernance exige une reddition de comptes régulière sur les aspects financiers et opérationnels, dont l'exactitude est attestée par un auditeur indépendant. La reddition de comptes suppose également l'imposition de pénalités ou de sanctions à ceux qui utilisent les ressources à des fins autres que les fins autorisées.

« La reddition de comptes est le processus suivant lequel les entités publiques et les personnes qui en font partie sont tenues de répondre de leurs décisions et de leurs actions, y compris en ce qui concerne l'utilisation des fonds publics et tous les aspects de la performance, et de se soumettre à un examen externe approprié. L'obligation de rendre compte repose sur une bonne compréhension des responsabilités par toutes les parties et une définition claire des rôles de chacun au moyen d'une structure solide. En fait, l'obligation

[2] International Federation of Accountants (IFAC), Corporate Governance in the Public Sector: A Governing Body Perspective, 2001.

de rendre des comptes consiste en l'obligation faite à une personne de répondre de l'exécution des responsabilités qui lui ont été confiées. [3]»

- **Prendre des mesures correctives.** Lorsque l'organisation n'a pas atteint les objectifs fixés sur le plan financier ou opérationnel, ou lorsque des problèmes sont décelés au chapitre du fonctionnement ou de l'utilisation des fonds, un système de gouvernance efficace permet d'identifier la cause des problèmes, de déterminer les mesures correctives à apporter et d'assurer un suivi pour établir si les mesures correctives ont été appliquées efficacement. **Les constatations et les recommandations des auditeurs** constituent des apports essentiels à une saine gouvernance qui peuvent inciter les organisations à prendre des mesures correctives promptes et appropriées pour pallier les faiblesses et les déficiences relevées.

- **Assurer la transparence.** Le principe de transparence concerne le degré d'ouverture de l'État envers ses citoyens.

Une bonne gouvernance comprend une communication adéquate des informations clés aux parties prenantes en ce qui concerne la performance et les activités de l'État. La transparence des actions et des informations du de l'Etat joue un rôle crucial dans la surveillance publique.

Les législateurs et le public comptent sur l'audit pour obtenir l'assurance que les actions du gouvernement sont éthiques et légales, et que les informations financières et opérationnelles reflètent avec exactitude la mesure réelle des activités.

- **Garantir la Probité**. Selon le principe de probité, les fonctionnaires doivent agir avec intégrité et honnêteté.

- **Promouvoir l'Équité.** Le principe d'équité concerne la mesure dans laquelle les représentants des organismes gouvernementaux font preuve de justice dans l'exercice des pouvoirs qui leur sont confiés (coût des services, prestations de service, forces publiques, et information).

[3]Source: IFAC, Governance in the Public Sector: A Governing Body Perspective, 2001.

3. Le Code de Bonnes Pratiques de Gouvernance des entreprises publiques de l'OCDE (2005) et à titre de droit comparé, celui du Burkina adopté en juin 2015

Les pratiques de bonne gouvernance reposent d'abord sur les dispositions légales et réglementaires (droit commun OHADA et réglementation spécifique nationale) qui doivent être strictement respectées aussi bien dans l'esprit, dans le contenu que dans la forme. Les lignes directrices de l'OCDE relatives à la gouvernance des entreprises publiques regroupent des règles de conduite et des recommandations complémentaires auxdites dispositions. Elles peuvent servir de source d'inspiration pour enrichir le contenu des textes en vigueur.

Ces lignes directrices font sienne la règle recommandée par l'OCDE de « *Comply or Explain* » (*appliquer la recommandation ou expliquer*) : Une fois adoptées, les entreprises publiques qui ne respecteront pas totalement ou partiellement l'une des recommandations du Code sont appelées à expliquer pourquoi elles y dérogent dans le chapitre« Gouvernance d'Entreprise » du rapport de gestion du Conseil d'administration et dans le rapport annuel sur le contrôle interne du PCA.

Il est évident que la mise en œuvre d'un tel Code commande une introspection des entreprises publiques sur elles-mêmes, laquelle suppose un processus de mise à niveau des ressources humaines et la mobilisation des moyens financiers nécessaires à l'amélioration de la qualité de production des informations à fournir par les dirigeants.

A titre de droit comparé, le Code de bonnes pratiques de gouvernance des sociétés d'Etat adopté en juin 2015 au Burkina comporte quatre (4) chapitres qui constituent les piliers d'un dispositif de bonnes pratiques de gouvernance des Sociétés d'État :

I. Rôle de l'Etat,
II. Responsabilité du Conseil d'administration et de la Direction générale,
III. Transparence et diffusion de l'information,
IV. Relations avec les Parties prenantes.

3.1 En ce qui concerne le rôle de l'Etat

Selon ce Code, le contrôle administratif et juridictionnel de l'Etat sur les Sociétés d'État gagnerait en efficacité avec :

- le renforcement et l'amélioration de la gouvernance de ces entités conformément aux recommandations du Code ;
- la responsabilisation des organes délibérants et de gestion par la contractualisation et l'obligation de rendre compte (contrat plan ou de programme, plan stratégique, contrats d'objectifs et programme annuel de performance, rapport annuel de performance) ;
- la rationalisation du contrôle externe public par l'introduction de l'audit basé sur les risques ;
- l'organisation de réunions périodiques de l'entité coordinatrice des Sociétés d'État avec les dirigeants des Sociétés d'État pour faire le point sur leurs performances et proposer des axes d'amélioration ;
- l'existence dans les Sociétés d'État d'une structure d'Audit interne, hiérarchiquement rattachée à la Direction Générale et rapportant au Conseil d'administration (via le Comité d'Audit) ;
- la transmission systématique du plan d'audit pluriannuel et annuel basé sur les risques et de tous les rapports des structures d'Audit Interne des Sociétés d'État au Conseil d'administration (Comité d'Audit) et aux corps de contrôle interne et externe (Autorité supérieure de contrôle d'Etat, Commissaire aux Comptes et Cour des Comptes) ;
- l'obligation pour chaque auditeur interne des Sociétés d'État de consacrer 40 heures au moins par an à sa formation continue ;

- la participation des responsables des structures d'Audit Interne des Sociétés d'État au Cadre de Concertation des Corps de Contrôle de l'ordre administratif ;
- la participation de l'entité coordinatrice des Sociétés d'État en tant qu'observateur au Cadre de Concertation des Corps de Contrôle de l'ordre administratif ;
- l'implémentation des rencontres d'échanges périodiques de l'entité coordinatrice avec les corps de contrôle interne et externe (IGF, Cour des Comptes) pour mieux adapter les stratégies et les actions d'encadrement et de conseil ;
- l'évaluation systématique du dispositif de management des risques au niveau des Sociétés d'État, des modalités de son implémentation comme outil de gouvernance stratégique et opérationnel.

3.2 En ce qui concerne la responsabilité du Conseil d'administration et de la Direction générale

Le Conseil d'administration a pour rôle, notamment, en plus des attributions classiques organisées par les textes fondateurs et le droit commun de l'OHADA :

- de veiller à ce que la société agisse dans le sens des missions qui lui ont été assignées et ce, en conformité avec la politique générale du Gouvernement et dans le respect des droits des autres Parties prenantes ;
- de définir les orientations stratégiques de la société, son mode de financement et sa politique de communication ;
- de conduire la procédure de recrutement du directeur général sous sa responsabilité, suite à un appel à candidature ouvert, transparent, objectif ;
- d'être impliqué après appel à candidature ou tout autre moyen légal de sélection objectif et transparent, au recrutement du directeur général et de proposer, le cas échéant, sa révocation ;
- d'apprécier la gestion des organes de direction des SE à travers la qualité du contrôle interne, du contrôle de gestion, les réalisations budgétaires, des coûts et prix de revient et sur la base de critères de performances ;
- de rendre pleinement compte et assumer les résultats de la société ;
- de mettre en place des comités spécialisés ;
- d'arrêter les comptes et procéder à une évaluation de ses performances (rapports annuels de gestion et sur le contrôle interne) ;
- de diligenter les contrôles et vérifications qu'il juge opportuns ;
- faire appel si nécessaire à des experts pour l'aider dans sa mission.

Dans ce cadre, le Conseil d'administration doit :

- exercer ses fonctions en toute objectivité et indépendance ;
- assurer l'accès à l'information et à la formation des Administrateurs et à l'évaluation de leur contribution individuelle et collective ;
- examiner les actes fondamentaux, conformément à la réglementation en vigueur, notamment, le plan stratégique pluriannuel, les contrats de performance, le budget, l'organigramme, le manuel des procédures, la cartographie des risques, le statut du personnel, le plan pluriannuel d'Audit Interne basé sur les risques, les emprunts et l'affectation des résultats ;
    - porter conseil aux dirigeants des SE ;
    - affirmer le caractère collégial des décisions prises et de la responsabilité qui s'y attache. Tous les Administrateurs doivent avoir les mêmes droits et les mêmes obligations.

Le rôle, responsabilités et relations du directeur général de la SE

Pour permettre d'évaluer la qualité de la gestion et les performances de l'équipe dirigeante, le Conseil d'administration conclura avec le directeur général de la société, à l'occasion de sa nomination, annuellement, et à des étapes importantes de la vie de l'organisme, notamment la recapitalisation de la société, l'adoption d'un contrat plan (ou de programme) ou d'un plan de restructuration, l'ouverture du capital au secteur privé, **un contrat d'objectif,**

précisant les attentes envers l'organisme ainsi que les orientations générales qui lui sont fixées.

Sur la base de ce contrat d'objectif (ou contrat de performance), le dirigeant concerné est tenu de décliner ces orientations générales en plan d'entreprise soumis à l'approbation du Conseil d'administration qui est appelé à évaluer régulièrement, notamment au moment de l'arrêté des comptes, la mise en œuvre de ce plan et d'effectuer les recadrages nécessaires. Ainsi, sur la base des objectifs généraux, la direction générale détermine les objectifs spécifiques, affecte les moyens et contrôle les résultats des directions et services opérationnels chargés de la mise en œuvre du plan d'entreprise. Il s'assure du respect des dispositifs de contrôle interne et de contrôle de gestion.

Ces résultats, mesurés notamment par des indicateurs de performance, font l'objet d'évaluation régulière et donnent lieu à **un rapport de performance** élaboré en fin d'année par la direction générale et **présenté au Conseil d'Administration.**

Les Comités spécialisés du Conseil d'administration

Il est recommandé au Conseil d'administration d'instituer autant de comités et de commissions spécialisés que cela est nécessaire. Il lui appartient également de fixer le nombre et de déterminer la structure et l'organisation de ses comités.

Le Conseil d'administration peut notamment décider de la mise en place des comités suivants :

- un Comité d'Audit,
- un Comité de la Stratégie et des Investissements,
- un Comité des Recrutements et des Rémunérations,
- etc.

Le Comité d'Audit est l'émanation du Conseil d'administration de la société et a pour mission :

- d'examiner le projet d'arrêté des comptes sociaux et d'évaluation des risques ;
- d'informer le Conseil d'administration des risques majeurs qui peuvent compromettre l'atteinte des objectifs de gestion ;
- d'apprécier à travers les opérations d'audit (interne et externe), la régularité des opérations, la qualité de l'organisation, la fiabilité et la bonne application du système d'information ainsi que les performances de la société ;
- de faire prescrire et de réaliser, aux frais de la société, les audits externes ainsi que les évaluations qui lui paraissent nécessaires. Le Comité d'Audit peut s'il le souhaite, solliciter des audits internes ou des expertises externes ou inviter tout expert indépendant à participer à ses travaux.

3.3 En ce qui concerne la transparence et la diffusion de l'information

Informations sur le contrôle interne, la gestion des risques et les transactions

La SE est tenue d'informer le public et les actionnaires sur :

- les dispositifs de contrôle interne et les procédures de diffusion des informations financières ;
- le fonctionnement des organes du Conseil d'administration ;
- les facteurs de risques significatifs ainsi que les mesures prises pour y faire face ;
- les aides financières éventuelles, notamment les garanties reçues de l'Etat et les engagements pris par l'Etat pour le compte des Sociétés d'État ;

- toute transaction significative avec des parties apparentées ;
- un rapport présenté par le PCA sur le contrôle interne et les informations significatives est transmis au Commissaire aux Comptes et à l'AG - SE.

Les SE doivent mettre en place et développer des dispositifs de contrôle interne et de gestion des risques

La mise en place de dispositifs efficients de contrôle interne est nécessaire pour ajouter de la valeur à l'activité de la société et l'aider à atteindre ses objectifs.

Ce dispositif doit comporter, notamment :

- un Code de déontologie et d'éthique des Employés (en annexe 2 du Code) ;
- un contrat plan (ou contrat de programme) ;
- un plan stratégique et opérationnel mis en œuvre par la contractualisation ;
- un plan annuel de passation des marchés ;
- un organigramme de gestion avec des fiches de description de poste ;
- un statut du personnel incluant des critères de recrutement et des procédures d'évaluation du personnel fondées sur les performances ;
- un référentiel des emplois et des compétences ;
- un règlement intérieur du personnel ;
- un plan de carrière du personnel ;
- un bilan social (contenu détaillé en annexe 5 du Code) ;
- un plan de formation pluriannuel du personnel ;
- une cartographie des risques majeurs et un plan de mitigation tenant compte du niveau d'appétence pour le risque du management ;
- un manuel des procédures à jour couvrant toutes les fonctions et un référentiel de contrôle interne ;
- un système d'information automatisé et intégré de gestion performant (comptabilité générale, budgétaire, matières, analytique, tableaux de bord de pilotage), permettant l'établissement et la publication d'états de synthèse réguliers, sincères et certifiés par un ou plusieurs auditeurs externes habilités à exercer la profession de Commissaire aux Comptes ;
- une structure de contrôle interne et de gestion (et de management des risques) et d'Audit Interne (intervenant sur la base d'un plan d'audit pluriannuel basé sur l'analyse des risques rapportant au Conseil d'administration).

La mise en œuvre de ce dispositif de premier et de second niveau de contrôle permettra d'optimiser l'atteinte des objectifs de gestion par la maîtrise des risques. **Il est recommandé également, à titre de bonnes pratiques, de produire en plus du rapport de gestion, un rapport sur le contrôle interne[4], structuré comme suit :**

I. Limitations éventuelles des pouvoirs du directeur général,
II. Préparation et organisation des travaux du Conseil d'administration :
    a. Composition du Conseil d'administration, mandats, durée des fonctions et indépendance,
    b. Fonctionnement du Conseil d'administration :
        i. Responsabilités et prérogatives du Conseil d'administration,
        ii. Fréquence et teneur des réunions,
        iii. Tenue des réunions :
            1. Convocation des Administrateurs,
            2. Accès à l'information,
            3. Communication régulière,
            4. Procès-verbaux des réunions.

    c. Règles et principes arrêtés pour les rémunérations de toute nature accordées aux mandataires sociaux
        i. Rémunération des membres du Conseil d'administration,

[4] Rapport présenté par le président du Conseil d'administration

ii. Rémunération des mandataires sociaux.

III. Procédures de contrôle interne
   a. Les objectifs du contrôle interne (enjeux),
   b. Principes et organisation de la SE,
   c. Evaluation et gestion des risques :
      i. Couverture des risques opérationnels,
      ii. Responsabilité juridique.
   d. Procédures relatives à l'information financière et comptable :
      i. Orientation,
      ii. Acteurs impliqués,
      iii. Calendrier des reportings,
      iv. Activités du Comité d'Audit :
         1. Composition,
         2. Attributions,
         3. Modalités de fonctionnement.
      v. Autres procédures :
         1. Santé et sécurité,
         2. Investissements et achats.

   e. Emprunts contractés par la société sur l'exercice et les conditions financières de ceux-ci.

   f. Transactions significatives avec des parties apparentées.

   g. Aides financières, notamment les garanties reçues de l'Etat et les engagements pris par l'Etat pour le compte de la société sur l'exercice.

   h. Honoraires et commissions versés à des tiers au cours de l'exercice, avec indication, pour chacun des 20 bénéficiaires les plus importants :
      i. Du nom du prestataire ou du bénéficiaire,
      ii. Des montants versés,
      iii. De la nature des prestations effectuées,
      iv. Du mode de contractualisation.

   i. Dons et transactions assimilées, avec des précisions sur la nature, les montants et les bénéficiaires.

   j. Les conventions règlementées

IV. Conclusion.

Mécanismes pour garantir la fiabilité de l'information

La fiabilité de l'information tout en étant en priorité garantie par une comptabilité fiable et un contrôle régulier par le Commissaire aux Comptes, peut aussi se faire valoir à travers les instruments et mécanismes suivants :

- la vérification des comptes effectuée annuellement par un Commissaire aux Comptes indépendant et compétent qui émet un avis externe et objectif sur l'image fidèle du patrimoine, la situation financière et les résultats de la société ;
- le Commissaire aux Comptes effectue sa mission conformément à la réglementation, aux diligences et normes professionnelles prescrites ;
- conformément aux Principes de gouvernement d'entreprise, à l'instar des organismes faisant appel à l'épargne et les Sociétés cotées, la durée du mandat du ou des Commissaires aux Comptes des Sociétés d'État **est fixée à 3 ans** et son caractère renouvelable s'inscrit dans la garantie de l'indépendance de l'auditeur externe. La rotation des Commissaires aux Comptes **tous les deux mandats** ainsi que le décalage dans le temps de l'échéance de leurs mandats doivent être privilégiés par la société, sans que cela ne contrevienne aux règles de la concurrence.

3.4 En ce qui les relations avec les parties prenantes

La relation SE – salariés

Dans le respect de la législation en vigueur, les principes suivants doivent encadrer la relation souhaitée entre la société et ses salariés :

- le respect du droit du salarié à la sécurité, à la sûreté, au respect de sa vie privée et à l'exercice des libertés fondamentales (expression, opinions, croyances) ;
- le respect de la liberté syndicale ;
- la non-discrimination dans l'emploi, la profession et la promotion de l'égalité ;
- la valorisation des emplois et des compétences et le renforcement de la formation et de la qualification des salariés ;
- le cadre de gestion des carrières, sa transparence et son accessibilité ;
- l'encouragement des salariés à se conformer aux principes de transparence, d'intégrité et d'éthique au sein de l'entreprise et la mise en place des mécanismes et mesures nécessaires pour assurer la protection aux salariés qui dénoncent d'éventuels actes de corruption ou de fraude, conformément à la législation en vigueur en la matière.

La relation SE- Environnement d'affaires

La Société d'État doit notamment veiller à mettre en œuvre les instruments et les politiques permettant l'atteinte des objectifs suivants :

- prévenir les risques liés à la sécurité des produits et à l'information fournie aux partenaires commerciaux ;
- prendre en compte les intérêts des parties dans la définition et l'exécution des clauses contractuelles ;
- prévenir les pratiques anticoncurrentielles ;
- mettre en place des systèmes de veille, de qualité, de traçabilité, d'alerte, de blocage, de retrait et de rappel des produits défectueux, le cas échéant ;
- éviter les conflits d'intérêt et la corruption active ou passive d'acteurs privés comme d'agents publics et dénoncer les éventuels actes frauduleux ou de corruption.

Les résultats escomptés sont :

- le renforcement des règles encourageant le libre jeu de la concurrence en favorisant une compétition plus large entre les soumissionnaires par la procédure d'appel d'offres comme règle générale ;
- la mise en place d'outils permettant de garantir la transparence dans la préparation, la passation et l'exécution des marchés ;
- l'adoption du principe d'égalité de traitement des soumissionnaires dans toutes les phases de passation des marchés ;
- la mise en place de procédures pour la performance de la dépense des SE par une détermination aussi exacte que possible des spécifications techniques par référence aux normes, par le remplacement de la règle du moins disant par celle du mieux disant pour un meilleur rapport qualité/prix et par l'introduction de mesures pour le suivi et l'évaluation des marchés ;
- le renforcement des règles d'éthique, de déontologie et la moralisation en introduisant des mesures de nature à supprimer les possibilités de recours à des pratiques de fraude ou de corruption ;
- la dématérialisation des procédures ;
- l'utilisation de voies de recours et de règlement, à l'amiable, des litiges concernant la passation des marchés.

La Responsabilité Sociale des Entreprises (RSE)

La RSE peut se traduire au niveau de la société par :

- la mise en place d'un Code d'éthique et de déontologie des Employés de la société,
- la non admission du travail des enfants, du travail forcé,
- la mise en place de programmes d'actions,
- une surveillance accrue des principes de sécurité (gestion des risques),
- des programmes d'assurance qualité, avec la mise en œuvre de nouvelles normes,
- une communication interne et externe, archivage,
- une veille éthique, sociétale et environnementale.

FICHE N°3 Le cadre de référence relatif au management des risques du COSO2

1. Le management des risques : définition et implications

Le Committee of Sponsoring Organizations of the Treadway Commission (COSO 1, 1992) définit le risque comme *«... la possibilité qu'un événement se produise et ait une incidence défavorable sur la réalisation des objectifs».*

Le management des risques, qui est étroitement lié au gouvernement d'entreprise, ***est le processus conduit par la direction qui consiste à comprendre les incertitudes (risques et opportunités) qui pourraient influer sur la capacité de l'organisation à atteindre ses objectifs, et à agir en conséquence.***

Il y a lieu de retenir de la définition que :

- **Le risque est la possibilité de survenance d'un événement incertain** qui entravera la réalisation des objectifs (fraude par exemple)
- L'opportunité désigne la possibilité de survenance **d'un événement qui favorisera la réalisation des objectifs**
- Le risque commence avec la formulation de la stratégie et la définition des objectifs
- Les risques sont inhérents à tous les aspects de la vie

À la lumière de cette définition du risque, il devient évident qu'une organisation rencontre un grand nombre de risques lorsqu'elle s'efforce d'appliquer sa stratégie et d'atteindre ses objectifs.

Cette multitude de risques pouvant entraver significativement la bonne marche de l'organisation, il apparaît d'autant plus nécessaire de disposer d'un processus qui permette de comprendre et de gérer efficacement les risques sur l'ensemble de l'organisation : Tel est le but du management des risques de l'entreprise (Enterprise Risk Management, ERM adopté par l'INTOSAI en 2007).

2. Le COSO1- 2013

2.1. Définition du contrôle interne selon le COSO 2013

Le contrôle interne est un processus mis en œuvre par le conseil, le management et les collaborateurs, et qui est destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité.

Loi Organique n°2014-337 du 5 juin 2014 portant Code de Transparence dans la Gestion des Finances Publiques :
Article 62 : Le **Contrôle Interne** désigne le système global de contrôle qui s'exerce au sein de l'Administration par ses services, visant à assurer une bonne application de la réglementation et des procédures en matière financière. **Il consiste en des vérifications systématiques et permanentes intégrées dans le système d'exécution de la dépense publique**

2.2. Les 17 principes structurants du COSO 2013

Les 5 composantes de la version initiale du COSO sont ici officiellement déclinées en 17 principes complétés par des points d'attention et des illustrations. Le tableau ci-dessous précise ces principes de base.

Les 17principes du COSO1 actualisé **2013, entré en vigueur le 15 décembre 2014**

Composantes	Principes	
Environnement de contrôle	**1**	L'organisation démontre son engagement en faveur de l'intégrité et de valeurs éthiques.
	2	Le conseil d'administration (Instances dirigeantes) fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne.
	3	La direction, agissant sous la surveillance du conseil (Instances dirigeantes), définit les structures, les rattachements, de contrôle ainsi que les pouvoirs et les responsabilités appropries pour atteindre les objectifs.
	4	L'organisation démontre son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs.
	5	L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne.
Evaluation des risques	**6**	L'organisation spécifie les objectifs de façon suffisamment claire pour permettre l'identification et l'évaluation des risques associés aux objectifs.
	7	L'organisation identifie les risques associés à la réalisation de ses objectifs dans l'ensemble de son périmètre de responsabilité et elle procède à leur analyse de façon à déterminer les modalités de gestion des risques appropriées.
	8	L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles de compromettre la réalisation des objectifs.
	9	L'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle interne.
Activités de contrôle	**10**	L'organisation sélectionne et développe les activités de contrôle qui contribuent à ramener à des niveaux acceptables les risques associés à la réalisation des objectifs.
	11	L'organisation sélectionne et développe des activités de contrôle général en matière de système d'information pour faciliter la réalisation des objectifs.
	12	L'organisation met en place les activités de contrôle par le biais de directives qui précisent les objectifs poursuivis et de procédures qui mettent en œuvre ces directives.
Information et communication	**13**	L'organisation obtient ou génère puis utilise des informations pertinentes et de qualité pour faciliter le fonctionnement des autres composantes du contrôle.
	14	L'organisation communique en interne les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne, notamment en ce qui concerne les objectifs et les responsabilités associés au contrôle interne.
	15	L'organisation communique avec les tiers au sujet des facteurs qui affectent le bon fonctionnement des autres composantes du contrôle interne.
Pilotage	**16**	L'organisation sélectionne, met au point et réalise des évaluations continues et/ou ponctuelles afin de vérifier si les composantes du contrôle interne sont bien mises en place et fonctionnent.
	17	L'organisation évalue et communique les faiblesses de contrôle interne en temps voulu aux responsables des mesures correctrices, notamment à la direction générale et au conseil d'administration (Instances Dirigeantes).

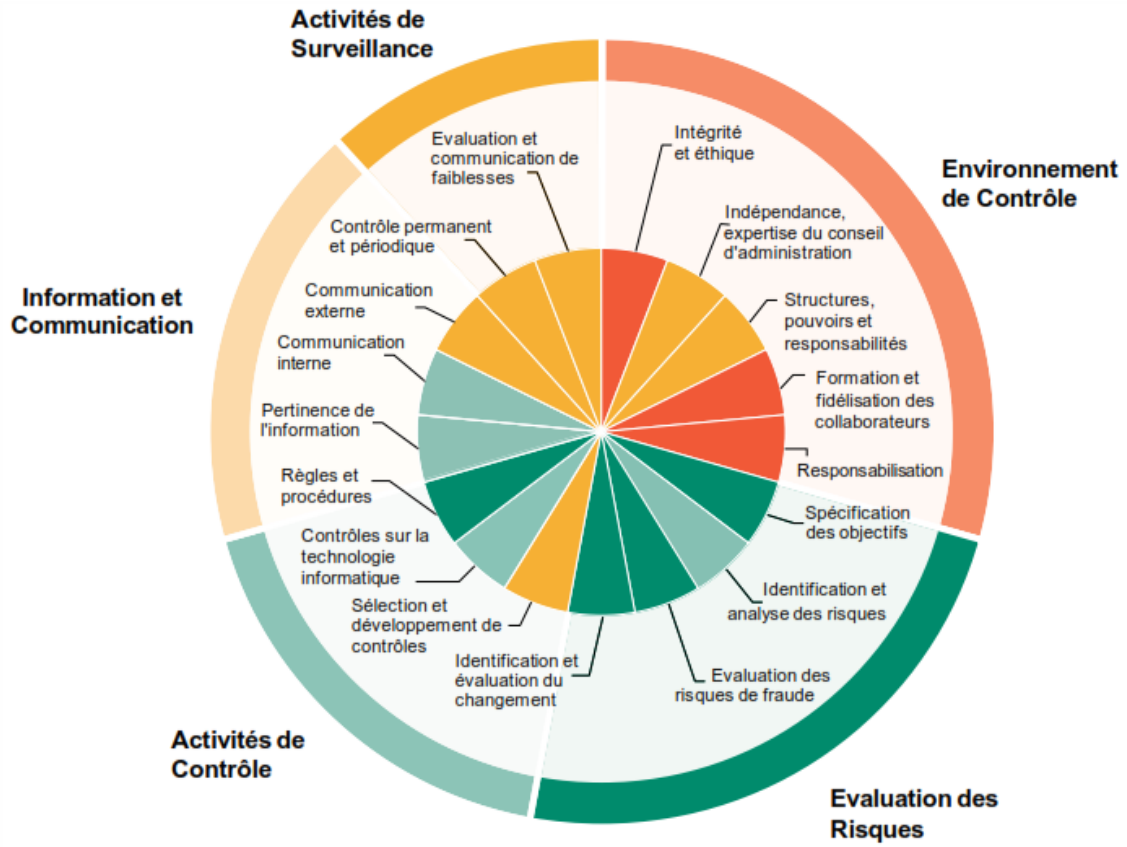
Les fondamentaux du référentiel COSO-I1992 n'ont pas changé. La définition du contrôle interne, les trois objectifs poursuivis et les cinq composantes dans lesquelles se répartissent les dispositifs de contrôle à mettre en œuvre sont conservés. La principale nouveauté réside dans ces 17 principes et les points d'attention associés. La version initiale de 1992 laissait aux responsables chargés de la mise en œuvre du contrôle interne l'initiative de décliner la nature des différents dispositifs à créer au sein de chacune des 5 grandes composantes du contrôle interne. Sans pour autant constituer un cadre rigide, la nouvelle version apporte à ce niveau une aide indiscutable en guidant l'expert du contrôle interne dans sa mise en œuvre.

2.3. Quelles actions sont à envisager pour se mettre en conformité avec le COSO 2013 ?

Pour se mettre en conformité, l'organisation peut :

- Faire un diagnostic sur la base des 17 principes pour identifier les axes d'amélioration nécessaires au niveau du groupe et des entités ;
- Approfondir certains sujets sur la base des 17 principes (par exemple la prise en compte des tiers dans l'évaluation du contrôle interne, l'utilisation des nouvelles technologies, notamment en ce qui concerne la sécurité des bases de données et le cloud-computing qui peut connaître une défaillance, etc.).

Et cela tout en veillant à l'articulation effective de ces 17 principes.



3. Les référentiels ou cadre conceptuel de management des risques du COSO2

COSO est l'acronyme abrégé de Committee Of Sponsoring Organizations of the Treadway Commission une commission à but non lucratif qui a établi en 1992 une définition standard du contrôle interne et crée un cadre pour évaluer son efficacité. Par extension ce référentiel s'appelle aussi COSO (COSO 1- 2013[5]).

Publié en 2004 et traduit en français par l'IFACI et price water house Coopers en 2005 **sous le titre *Le Management des risques de l'entreprise, Cadre de référence - Techniques d'application,*** *l*e COSO 2 **est un cadre de référence international solide permettant d'aider les organisations à identifier, évaluer et gérer efficacement le risque.**

L'INTOSAI a adopté le COSO 2 en 2007, voir normes de contrôle interne à promouvoir dans le secteur public - *Informations complémentaires sur la gestion des risques des entités* de l'INTOSAI : INTOSAI GOV 9130

⇨Un peu d'histoire

En réponse à une série de scandales financiers intervenus dans les années 80 aux USA (Polly Peck, Maxwell, et Barings,), des spécialistes de cabinets d'audit et d'expertise comptable ainsi que des chercheurs se sont réunis en 1985 à la demande du sénateur américain Treadway sur le thème de la « fraude dans le reporting financier ».

⇨La commission Treadway était chargée :

- d'étudier les déterminants des principales causes de fraudes dans les états financiers
- et de formuler des recommandations pertinentes.
- Le rapport de la commission Treadway est publié en septembre 1987.
- Il constitue une base de recommandations pour prévenir et détecter les fraudes dans les états financiers.
- Après la publication du rapport Treadway, la commission COSO a été constituée pour poursuivre la mise en œuvre ses recommandations.

⇨Les organisations qui ont sponsorisé les travaux du COSO sont :

- American Accounting Association (AAA): Association Comptable Américaine
- American Institute of Certified Public Accountants (AICPA): Institut des experts-comptables
- Financial Executives International (FEI): La fédération internationale des Directeurs financiers
- Institute of Management Accountants (IMA): l'institut des professionnels comptables et financiers d'entreprise
- Institute of Internal Auditors (IIA): Institut des auditeurs internes
- Le COSO est indépendant des organisations membres.
- Sur la base des recommandations de la commission Treadway le COSO a rédigé le «**Internal Control – Integrated Framework**» - cadre conceptuel du contrôle interne intégré - ou référentiel COSO publié en 1992 (COSO 1).
- Le COSO 1 propose un cadre de référence pour la gestion du contrôle interne.

Le COSO laisse à disposition le référentiel de 1992 jusqu'au 15 décembre 2014, date à laquelle il sera retiré du marché et définitivement remplacé par la mise à jour de 2013.

3.1 Définition du management des risques par le COSO 2

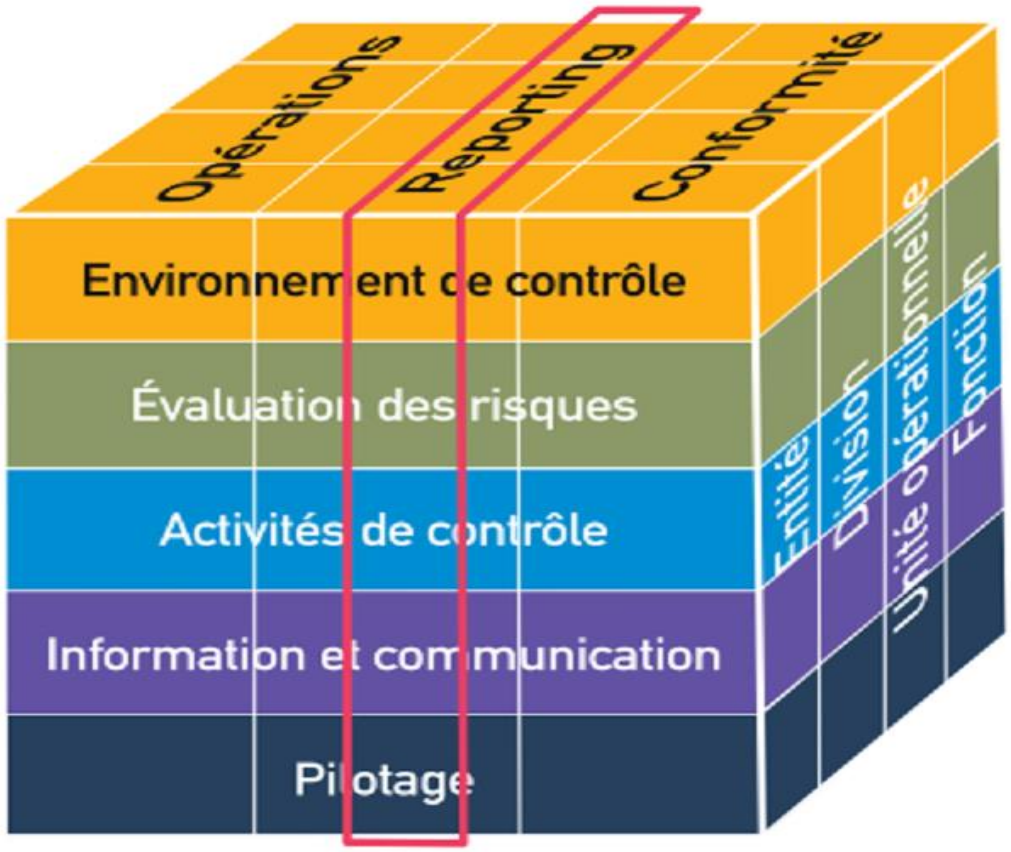
⇨Le COSO 1 révisé en 2013 **(COSO 2013): Cadre de référence pour l'évaluation du contrôle interne**

[5] Adopté par l'INTOSAI

C'est le processus mis en œuvre par la direction générale, la hiérarchie, le personnel d'une entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- La réalisation et l'optimisation des opérations,
- La fiabilité des informations,
- Respect des réglementations en vigueur,
- La protection des ressources.

➪ Le Référentiel de Base – Le Modèle COSO1 révisé en 2013 - le cube à 3 dimensions



Les 3 Objectifs :

- Rendre compte
- Conformité
- Opérations

Les 5 Composantes :

- **Environnement de contrôle** (culture du contrôle, éthique et style de management, engagement de la direction,…)
- **Evaluation des risques** (définition des objectifs, identification et évaluation des risques, y compris le risque de fraude, plans d'actions pour les maîtriser…)
- **Activités de contrôle** (Contrôle sur la technologie, s'assurer de la correcte application des directives, maîtriser les risques, gestion des changements…)
- **Information et communication** (interne, externe, informelle, formelle,…)
- **Pilotage** (pilotage de gestion, évaluation et autoévaluation, organes de contrôle)

NB: INTOSAI a adopté le COSO (2013 et 2).

En 2002, le Congrès américain, en réponse à d'autres scandales financiers et comptables (Enron, Worldcom, ...), promulgue la loi Sarbanes–Oxley (the Sarbanes-Oxley Act ou SOXAct).

Cette loi oblige les sociétés faisant appel à l'épargne publique à évaluer leur contrôle interne et à en publier leurs conclusions.

Imposant en outre l'utilisation d'un cadre conceptuel, le SOX Act a favorisé l'adoption du COSO comme référentiel.

En France, la loi LSF (Loi de sécurité financière) promulguée peu après en 2003, a également contribué à sa diffusion.

3.2 Le cadre de référence ou conceptuel du management des risques COSO 2 (Enterprise Risk Management Framework)

Le référentiel initial appelé COSO 1-1992 a évolué depuis 2002 vers un second corpus dénommé *COSO 2*. **Le « coso 2 » est une étude réalisée à la suite de Sarbanes-Oxley Act (SOX).**

Il ne propose pas un référentiel de Contrôle Interne (à l'instar du COSO1 révisé en 2013) mais un modèle de gestion des risques.

Ainsi le COSO 2 propose un cadre de référence pour la gestion des risques de l'entreprise (Enterprise Risk Management Framework). **Il s'appuie sur le COSO1 révisé en 2013 (COSO 2013) comme référentiel de Contrôle Interne.**

⇨Le système de management des risques de l'entreprise, c'est quoi ?

- **Le COSO2 définit le management des risques de l'entreprise comme :** « Le processus mis en œuvre par le Conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence au risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation. »

Il apparaît que **le COSO 2 inclut les éléments du COSO1-2013** et est basé essentiellement sur une vision orientée risques de l'entreprise.

☛ La définition ci- dessus très large reflète certains concepts fondamentaux.

Le dispositif de management des risques :

- est un processus permanent qui irrigue toute l'organisation,
- est mis en œuvre par l'ensemble des collaborateurs, à tous les niveaux de l'organisation,
- est pris en compte dans l'élaboration de la stratégie,
- Est mis en œuvre à chaque niveau et dans chaque unité de l'organisation et permet d'obtenir une vision globale de son exposition aux risques (cartographie)

Est destiné à :

- identifier les événements potentiels susceptibles d'affecter l'organisation,
- et à gérer les risques dans le cadre de l'appétence pour le risque
- Donne à la direction et au conseil d'administration une assurance raisonnable (quant à la réalisation des objectifs de l'organisation)

- Est orienté vers l'atteinte d'objectifs des différentes unités

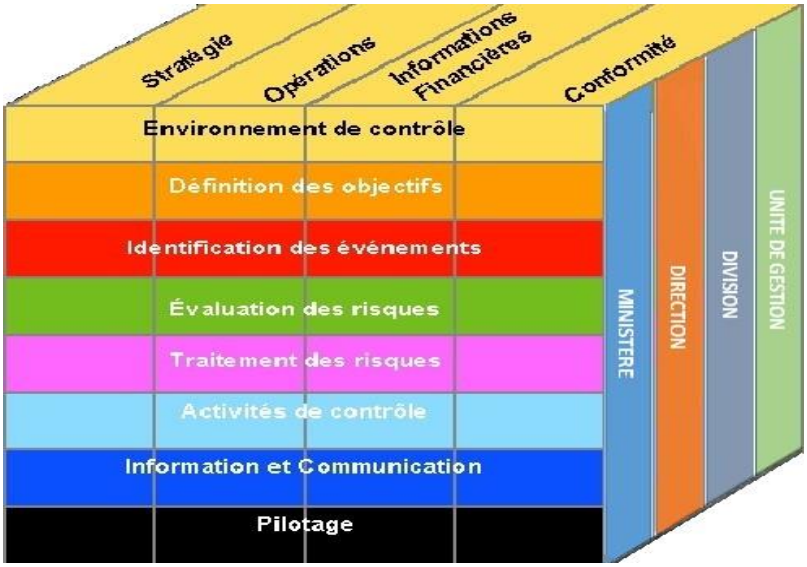
Le cadre de référence de management du risque (COSO 2) est la base du ERM et de l'ABR.

La définition intègre les principaux concepts sur lesquels s'appuient les organisations pour définir leur dispositif de management des risques et se veut une base pour la mise en œuvre d'un tel dispositif au sein :

- d'une organisation,
- d'un secteur industriel,
- ou d'un secteur d'activité.

⇨Cadre de Référence du management des risques de l'entreprise (le COSO 2)

☛Le cadre de référence du ERM se présente toujours en cube à 3 dimensions, mais réaménagé pour intégrer le risque



L'Enterprise Risk Management identifie :

- 8 composants
- et 4 objectifs de contrôle interne

Les 8 composantes sont:

1. environnement de contrôle,
2. fixation des objectifs,
3. identification des événements,
4. évaluation des risques,
5. traitement des risques,
6. activités de contrôle,
7. information et communication,
8. pilotage.

Nota : la composante « Evaluation des risques » du COSO – 1 (révisé en 2013) est déclinée dans le COSO – II en quatre (4) items qui précisent cette notion :

1. la fixation des objectifs,
2. l'identification des événements,
3. l'évaluation des risques,
4. le traitement des risques,

Les 4 objectifs sont d'ordre:

- **stratégiques (s'ajoute aux 3 objectifs de COSO – 1),**
- opérationnels,
- Rendre compte (reporting),

- et conformité (et sécurité des actifs).

1. Le cadre de référence ERM : vise l'atteinte des objectifs

☛Les 4 grandes catégories d'objectifs de l'entité sont représentées par des colonnes :

- **stratégiques**
- Opérationnels
- Reporting
- Conformité (et
- Sécurité actif)

➥L'organisation ayant le contrôle sur :

- les objectifs relatifs à la fiabilité du reporting.
- et à la conformité aux lois et aux règlements, il est légitime d'attendre du processus de management des risques une assurance raisonnable quant à l'atteinte de ces objectifs.
- Cependant, l'atteinte des objectifs stratégiques et opérationnels dépend parfois d'événements extérieurs qui peuvent échapper au contrôle de l'organisation.
- Par conséquent, le management des risques ne peut donner qu'une assurance raisonnable que le management est informé en temps utile de l'état de progression de l'organisation vers l'atteinte de ses objectifs.

2. Le cadre de référence du ERM prend en compte les activités à tous les niveaux de l'organisation :

- L'entité ou le Ministère,
- Les Directions,
- Les divisions
- Les unités de gestion.

Il est demandé à l'organisation d'avoir une vision de ses risques sous forme d'un portefeuille.

Ce portefeuille doit caractériser les risques à chaque niveau de l'organisation :

- La compilation du portefeuille permet donc d'avoir une vision globale des risques de l'organisation.
- Cette vision pourra alors être rapprochée du "risque acceptable" défini pour l'organisation.

3. Les 8 composantes du cadre conceptuel (les lignes) interagissent entre eux …

1. Environnement interne
2. Définition d'objectifs
3. Identification des évènements
4. Évaluation des risques
5. Réponses aux risques
6. Activités de contrôle
7. Information et communication
8. Pilotage

⇨1. L'environnement de contrôle qui comprend :

- **La culture du risque,** qui représente la façon dont l'organisation appréhende les risques dans toutes ses activités.
- **L'appétence au risque,** ou l'appétit pour le risque, c'est-à-dire le niveau de risque global qu'une organisation accepte de prendre.
- **L'organe délibérant** de gouvernance qui oriente et supervise.
- **L'intégrité et les valeurs éthiques,** reflétant les choix, jugements de valeur et styles de management.
- **L'engagement de compétence,** portant sur les connaissances et les aptitudes nécessaires à l'accomplissement des tâches requises.
- **La structure organisationnelle,** à savoir l'infrastructure permettant de planifier, d'exécuter, de contrôler et de faire un suivi des activités.
- **La délégation de pouvoirs et de responsabilités,** pour aborder et résoudre des problèmes, ainsi que les limites des pouvoirs délégués.

- **La politique de ressources humaines,** qui englobe les activités relatives au recrutement, à la gestion de carrière, à la formation, aux évaluations individuelles, à la promotion, à la rémunération et aux actions d'amélioration.

⇨2. La fixation des objectifs

- La déclaration **de mission de l'entité définit dans les grandes lignes les objectifs qu'elle cherche à atteindre**.
- La stratégie mise en œuvre pour réaliser la mission et les objectifs correspondants est souvent plus dynamique que la mission et sera ajustée pour prendre en compte l'évolution des conditions.
- Les objectifs **opérationnels**, de **reporting** et de **conformité** découlent des objectifs définis au niveau **stratégique**.
- Les **objectifs doivent être alignés sur l'appétence au risque de l'organisation**, qui détermine le niveau de risques qu'elle accepte de prendre pour atteindre ses objectifs.
- **Les objectifs opérationnels représentant le point focal des ressources à affecter**, s'ils manquent de clarté ou sont mal conçus, ces ressources peuvent être mal affectées.

⇨3. L'identification des événements (ou risques)

- **Les événements sont des incidents ou des faits d'origine interne ou externe qui affectent la mise en œuvre de la stratégie ou la réalisation des objectifs.**
- Le management identifie les événements potentiels qui, s'ils se réalisent, pourront affecter l'organisation.
- Lors de la phase d'identification des événements, **le management prend en compte, à l'échelle de l'organisation dans sa globalité**, **différents facteurs externes et internes pouvant se traduire par des menaces et des opportunités.**

- **Les facteurs externes sont par exemple :**
  - **Economiques**, tels que les fluctuations de prix ;
  - **Environnementaux,** comme les inondations, les incendies, les séismes ;
  - **Politiques,** tels que l'élection, la promulgation de nouvelles lois et règlements ;
  - **Sociaux,** à savoir les évolutions démographiques, les coutumes sociales, les structures familiales ;
  - **Technologiques,** comme les nouveaux modes de commerce électronique, de stockage ou de traitement.

Nota :

- L'analyse PEST est un instrument utile pour comprendre et évaluer l'incidence de facteurs ***externes sur la réalisation des objectifs de l'entité.***
- PEST est un **acronyme désignant les facteurs :**
  - Politiques,
  - Economiques,
  - Sociaux,
  - et Technologiques.

- **Comme exemple de facteurs internes, on peut citer:**
  - **Les infrastructures :** augmentation des implantations à l'étranger.
  - **Le Personnel :** accidents du travail, fraude, grève.
  - **Processus :** modification, erreurs d'exécution ou externalisation.
  - **Technologie :** augmentation des ressources disponibles pour gérer la volatilité de la volumétrie opérationnelle, les violations de la sécurité ou l'interruption des systèmes.

- **Les techniques d'identification des événements sont à la fois :**
  - rétrospectives (passé, précédents):
    - •les rapports et les comptes annuels,
    - •les historiques de défauts de paiement et les rapports internes.
  - et prospectives (futur) :
    - •l'évolution démographique,
    - •les nouvelles conditions du marché,
    - •et les changements prévus dans l'environnement politique.

⇨4. L'évaluation des risques

- L'évaluation des risques consiste à déterminer dans quelle mesure des événements potentiels sont susceptibles d'avoir un impact sur la réalisation des objectifs.
- Le management évalue **la probabilité d'occurrence et l'impact de ces événements**
- Pour simplifier à l'extrême, le risque inhérent représente le risque « brut », tandis que le risque résiduel est le risque « net ».
- Le risque inhérent est celui auquel l'organisation est exposée en l'absence de mesures correctives prises par **le management pour en modifier la probabilité d'occurrence ou l'impact.**

Le Risque inhérent : l'exposition au risque qui existe avant prise en considération des mesures de contrôle interne. **Le Risque résiduel**: L'exposition au risque qui existe après considération des contrôles internes mis en place pour détecter ou prévenir ce risque.

- **Les risques** peuvent être mesurés en termes de:
  - **Probabilité**: Quelle est la probabilité que ce risque aura lieu et avec quelle fréquence?
  - **Impact**: Quelle est l'ampleur, la gravité, conséquence de cet événement?

- **Il existe de multiples méthodes pour évaluer l'impact et la probabilité d'occurrence d'un risque :**
  - recueil d'avis généraux et de points de vue de différentes personnes ;
  - utilisation de modèles probabilistes sophistiqués ;
  - benchmarking ;
  - l'entretien de créativité ou analyse pragmatique des risques (par la Méthode MIRIS Maîtrise Interne des Risques et Sécurité).

MIRIS : Une démarche tournée vers la maîtrise de tous les risques d'activités avec un retour sur investissement

➢ Etapes de réalisation :

1. Inventaire avec les managers et les opérationnels des missions et des objectifs de structures.
2. Recensement de l'ensemble des processus et des informations.
3. Travail de groupe de description chronologique :
   - Des objectifs stratégiques
   - Des objectifs opérationnels
   - Des activités et tâches (chronologique).
4. Identifier en groupe les risques potentiels pesant sur les tâches (facteurs d'empêchement internes et externes).
5. Déterminer la catégorie ou typologie de risque (sur 15 types).
6. Imaginer collectivement les causes probables (composant du contrôle interne).
7. Identifier collectivement les conséquences probables de la réalisation du risque.
8. Évaluer et classer chaque scenario de risque inhérent (probabilité x impact) en appliquant les barèmes de MIRIS.
9. Définir l'ensemble des bonnes pratiques de contrôle interne communément admises de maîtrise des risques qui devront exister.
10. Evaluer l'efficacité des parades ou CI en place en appliquant les barèmes de MIRIS.
11. Evaluer l'exposition résiduelle.
12. Identifier l'appétence au risque du management (niveau : Traiter, Tolérer, Transférer ou Terminer).
13. Déterminer le niveau de priorisation (échelle de 1 à 3) et classement du risque (déjà survenu : Oui/Non).
14. Proposer un plan de mitigation ou d'action (recommandation, responsables, période).

15. Proposer un plan stratégique d'audit interne, le cas échéant une mission d'audit (audit proposé, type, objectif, effort indicatif).

- **MIRIS introduit :**
  - Une approche participative et les collaborateurs doivent jouer le jeu de bonne foi.
  - Une méthode pragmatique apportant une solution à la recherche d'adéquation : enjeux – responsabilité (tout est supervisé).
- **Une démarche de changement :**
  - En changeant la confiance souvent aveugle envers le monde dans lequel on travail (pessimisme professionnel : remise en cause perpétuelle).
  - En changeant le savoir – faire par l'apport une méthodologie d'analyse professionnelle des risques.
  - En instituant une culture de partage (des connaissances, des savoir-faire).
  - En créant une synergie de groupe collaborant à une œuvre commune (référentiel de CI).
  - En amenant tous les acteurs à prendre leurs responsabilités, dans une culture d'auto-gestion et d'auto suggestion par la recherche de solutions adaptées.
- **MIRIS est donc un puissant levier de motivation (tout le monde est impliqué et a un rôle reconnu)**
- **MIRIS est également une démarche à forte valeur ajoutée parce qu'elle privilégie :**
  - avant les actions de communication et de formation,
  - Et par la suite les solutions organisationnel et enfin les moyens techniques.
- **Travers MIRIS, le CI devient un outil de management et de stratégie des entités.**

Nota :

- Les risques **inhérents sont évalués dans un premier temps**.
- Le risque résiduel sera évalué à partir des réponses du management.

⇨ 5 Le traitement des risques.

Une fois les risques évalués, le management détermine quels traitements appliquer à chacun de ces risques à partir de son niveau d'appétence au risque.

Les différentes solutions possibles sont selon le COSO :

- l'évitement (Abandon, **T**erminer) : pas toujours possible dans le secteur public.
- la réduction par le contrôle interne (**T**raiter) : action sur la probabilité ou l'impact.
- et l'acceptation ou **T**olérer (coût/avantage).
- le partage (**T**ransfert ou la sous traitance).

Toutefois, la plupart des risques ne pourront pas être entièrement transférés. En particulier, **il est généralement impossible de transférer le risque lié à la réputation** même dans le cas où le service à fournir a été externalisé.

Le choix doit porter **sur une solution ramenant le risque résiduel en deçà du seuil de tolérance souhaité par la direction**. Les opportunités potentielles sont également identifiées.

⇨ 6. Activités de contrôle (voir COSO1 révisé en 2013).

Les activités de contrôle sont **constituées de politiques et procédures *qui permettent de s'assurer que les traitements des risques souhaités par la direction ont été effectivement mis en place***. Les activités de contrôle **sont présentes dans toute l'organisation**, à tout niveau et dans toute fonction.

- Ces interventions sont :
  - Préventives, détectives ou de correctives (ou de protection),

- manuelles ou automatiques,
- et s'effectuent au niveau du processus ou au niveau du management.

- Quelques exemples des activités de contrôle les plus courantes décrites par le COSO :
  - **Revues du management**, tels les examens du respect du budget, l'actualisation des prévisions, la surveillance des actions ou des initiatives de maîtrise des coûts.
  - **Supervision directe d'une activité ou d'une fonction** par les responsables de fonctions ou d'activités spécifiques, par exemple vérification des rapports analytiques de gestion, rapprochements.
  - **Traitement de l'information.** Contrôles conçus pour vérifier l'exactitude, l'exhaustivité et la validation des transactions, tels que :
    - les contrôles généraux de l'infrastructure,
    - la sécurité physique et logique,
    - les contrôles sur la mise en œuvre des systèmes,
    - les évolutions de versions ou les modifications,
    - la reprise après sinistre et les contrôles des opérations issues des systèmes.

  - **Contrôles physiques :**
    - (1) l'inventaire physique des espèces, des titres, des stocks, du matériel et des autres immobilisations, et la comparaison du résultat de cet inventaire avec les chiffres enregistrés dans les comptes et les dossiers
    - et (2) les obstacles ou restrictions physiques, tels que les barrières et les verrous.
  - **Indicateurs de** performances : analyse des écarts entre prévisions et réalisations.
  - **Séparation des** tâches incompatibles afin de limiter le risque d'erreur ou de fraude.

⇨ 7. Information et communication.

Les **informations pertinentes** sont **identifiées, saisies et communiquées** dans un format et dans des délais permettant à chacun de s'acquitter de ses responsabilités. Elles doivent être suffisamment étoffées pour répondre aux besoins qu'a l'organisation de repérer, d'évaluer et de traiter le risque tout en restant dans ses différents niveaux de tolérance au risque.

- **Le COSO précise que l'information doit être :**
  - appropriée et aussi détaillée que nécessaire ;
  - disponible dès que nécessaire ;
  - actualisée, reflétant les données opérationnelles et financières les plus récentes ;
  - exacte et fiable ;
  - accessible à ceux qui en ont besoin.

- **Quant à la communication de l'information, elle peut revêtir des formes très diverses :**
  - manuels de politique de l'organisation (MPAFC),
  - notes internes,
  - courriers électroniques,
  - sites Internet et Intranet,
  - avis sur des panneaux d'affichage et messages vidéo.

⇨ 8. Pilotage

Le dispositif de management des risques fait l'objet d'un pilotage, qui repose sur l'évaluation de l'existence et du fonctionnement de ses éléments. Les opérations courantes de **pilotage s'inscrivent généralement dans le cadre des activités quotidiennes** du management. Les défaillances relevées grâce à ce pilotage sont remontées à la hiérarchie. Les problèmes les plus graves *sont portés à l'attention de la direction générale et du Conseil*.

- **En dehors des activités courantes de pilotage du management d'autres individus participent au processus de pilotage :**

- les auditeurs internes font partie du système global de pilotage, et les résultats de chaque audit permettent d'évaluer l'efficacité des activités de management des risques y afférentes.
- Par ailleurs les travaux des auditeurs indépendants extérieurs (comme les commissaires aux comptes) peuvent aussi influer sur l'évaluation par le management de l'efficacité de ses activités courantes de management des risques.

- **Les composants du dispositif de management des risques permettent de répondre à 5 questions courantes et quotidiennes :**
  - Qu'essayons-nous d'accomplir (quels sont nos objectifs) ?
  - Qu'est-ce qui pourrait nous empêcher de l'accomplir (quels sont les risques, quelle que soit leur gravité, et comment sont-ils susceptibles de se produire) ?
  - Quelles options avons-nous pour que cela ne se produise pas (quelles sont les stratégies de management des risques, donc les traitements disponibles) ?
  - Sommes-nous en mesure de mettre en œuvre ces options (avons-nous élaboré et instauré des activités de contrôle permettant de déployer les stratégies de management des risques) ?
  - Comment saurons-nous que nous avons atteint nos objectifs (existe-t-il des informations qui permettront d'attester de la réussite et pouvons-nous surveiller les performances de manière à vérifier que nous avons réussi) ?

3.3 Modèles de Contrôle – Une Approche du Risque et du Contrôle

- Pourquoi est-il important de mettre le risque au centre de la démarche d'audit?
- Introduit un langage commun entre la direction et l'auditeur concernant le risque et le contrôle
- Aide une organisation à mettre en œuvre des mesures de sauvegarde de 'bon sens'
- Aide à ce que le risque soit géré plus efficacement et mieux surveillé
- Aide à orienter l'activité d'audit et d'inspection vers les risques les plus significatifs

⇨ Les Points Communs des Référentiels

- La gestion du risque est une composante de base pour une gouvernance et un contrôle interne efficace.
- La gestion du risque est une responsabilité de la direction et du personnel.

Les auditeurs doivent inscrire leurs tâches sur la gestion des risques et le contrôle dans un dialogue continu avec les organes de direction et le personnel en respectant les principes d'indépendance et d'objectivité.

⇨ Exemples de Bonnes Pratiques dans le Secteur Public

- Pays ayant adopté ou mettant actuellement en œuvre COSO-I et/ou COSO-II au sein des services publics:
  - ✓ *Afrique du Sud, Kenya, Indonésie, Royaume-Uni, Canada, Mozambique, Burkina, Mali, Sénégal, Côte d'ivoire, Togo, Bénin….*
- Pays ayant adopté les normes d'Audit Interne IIA:
  - ✓ *Afrique du Sud, Kenya, Indonésie, Royaume-Uni, Canada, Ouganda, Burkina….*

⇨ Quelques Questions à Traiter au Cours de la séance

- Qu'entend-on par risque?
- Qu'entend-on par gestion des risques?
- Quelle est la responsabilité de la direction dans la gestion des risques?
- Pourquoi la gestion des risques est importante dans le secteur public?
- Pourquoi l'audit interne devrait-il être impliqué dans la gestion des risques?
- Pourquoi devrions-nous utiliser des 'principes' quand c'est plus facile de suivre des 'règles'?
- Comment réconcilier une culture de 'conformité' vers une culture 'de maîtrise des risques' et de performance.

4. Evolution des objectifs et des préoccupations de l'audit interne (domaines et sujets audités)

Avant — **Comptabilité** — **Finances** — **Administration** — **Aujourd'hui**

Tous les domaines :
Industriel
Commercial
Informatique
Social
Juridique
Fiscal
Ressources humaines
Communication
Environnement
Etc.

- Chiffres revus exacts, Procédures respectées
- Informations fiables, Procédures suffisantes, Actifs protégés

De l'Audit des comptes❶

- Organisation efficace
- Economie des moyens
- Célérité, fluidité
- Système d'information pertinent
- Responsabilités claires
- Recherche compétitive, Adaptabilité, flexibilité

A L'Audit des opérations❷

-
- Gestion des risques,
- Processus de contrôle
- Gouvernance

Puis à l'Audit de l'organisation et des risques❸

Aujourd'hui

FICHE N°4 — Rôle et responsabilités dans le cadre du dispositif de management des risques

1. Le Conseil exercera au mieux ses responsabilités de gouvernance en :

- Établissant un comité de gouvernance ;
- Précisant les exigences de reporting au Conseil ;
- Réévaluant régulièrement (tous les ans) les attentes vis-à-vis de la gouvernance ;
- Créant une structure organisationnelle qui vienne en appui à la réalisation de la stratégie de l'organisation ;
- Instaurant une politique de gouvernance concernant la réalisation des principales activités de l'organisation ;
- Définissant et mettant en place des lignes hiérarchiques claires en termes de responsabilité et de reddition des comptes, au sein de l'ensemble de l'organisation ;
- S'assurant d'une supervision adéquate par la direction, avec notamment l'instauration et le maintien d'un dispositif solide de contrôle interne.

2. La direction générale exercera ses responsabilités de gouvernance en :

- Instaurant un comité de gestion des risques (Comité de direction) ;
- Précisant les exigences de reporting (états financiers, opérationnel et tableau de bord) ;
- Communiquant les informations clés de manière appropriée et transparente aux parties prenantes ;
- Surveillant correctement les transactions et les situations potentiellement sources de conflit d'intérêts avec les parties liées ;
- Evaluant régulièrement (probablement tous les ans) les attentes concernant la gouvernance ;
- Cette situation donne également à la direction générale l'occasion d'évaluer l'efficacité globale du programme de management des risques de l'organisation ;
- Communiquant les processus de gouvernement d'entreprise et en comparant ces processus avec les codes nationaux et les bonnes pratiques reconnues.

3. Les propriétaires de risques

Le directeur général et les autres dirigeants sont les propriétaires des risques au sein de l'organisation.

Ils ont la responsabilité, au quotidien, de veiller à ce que les activités de management des risques permettent de gérer efficacement les risques conformément à l'appétence pour le risque de l'organisation dans la réalisation des objectifs.

4. L'audit interne est un acteur efficace du processus de gouvernance s'il :

- S'efforce de comprendre pleinement les orientations et les attentes du Conseil s'agissant du gouvernement d'entreprise.
- Soutient le programme de management des risques de la direction.
- **Elabore un plan d'audit interne** englobant les missions d'assurance concernant la gouvernance et prévoit des communications périodiques à la direction générale et au Conseil au sujet de l'efficacité des activités de management des risques.
- Les activités d'assurance internes et externes fournissent à la direction et au Conseil une assurance raisonnable quant à l'efficacité des activités de gouvernance : Ces intervenants sont notamment les auditeurs internes et les auditeurs externes indépendants.

Au total : Les Pré-requis de toute démarche d'audit:

⇨La connaissance des Normes d'audit:

- Normes de *Institute of Internal Auditors* – IIA ou Institut des auditeurs internes (www.theiia.org); normes de contrôle de l'INTOSAI, IFAC, …

⇨La maîtrise des Référentiels de contrôle interne et de management des risques

- COSO IC-IF, COSO ERM, ISO 31000, KING 3 pour la gouvernance des entreprises, INTOSAI, AMF,…

Le cadre conceptuel peut être défini comme un ***ensemble structuré d'objectifs et de principes fondamentaux*** liés entre eux et permettant de mettre au point des normes cohérentes.

Le cadre conceptuel éclaire la ***signification des normes et les limites de leur validité***.

Questions à choix multiple (à Traiter en groupe : durée 1 heure)

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Selon le référentiel de contrôle interne du COSO 2013, tous les éléments suivants font partie de l'environnement interne de contrôle d'une organisation sauf un, lequel ?
   a. Fixer les objectifs de l'organisation.
   b. Engagement du management en faveur de l'intégrité et de valeurs éthiques.
   c. Assigner des pouvoirs et des responsabilités.
   d. Engagement du management en faveur de la compétence.

2. Parmi les éléments suivants, lequel ne constitue pas un exemple de stratégie de partage des risques ?
   a. Externaliser un domaine à haut risque non essentiel.
   b. Vendre une unité non stratégique.
   c. Se couvrir contre les fluctuations des taux d'intérêt.
   d. Souscrire une police d'assurance pour se protéger contre les aléas météorologiques.

3. Une organisation surveille un site Web qui accueille des blogs anonymes consacrés à son secteur d'activité. Récemment, des messages anonymes ont évoqué l'adoption éventuelle d'une législation susceptible d'avoir un effet considérable sur le secteur en question. Parmi les éléments suivants, lequel pourrait engendrer le risque le plus élevé si cette organisation prenait des décisions fondées sur les informations contenues sur ce site Web ?
   a. La pertinence de l'information.
   b. La disponibilité de l'information en temps utile.
   c. L'accessibilité de l'information.
   d. L'exactitude et la fiabilité de l'information.

4. Qui est responsable de la mise en œuvre du management des risques ?
   a. Le directeur financier.
   b. Le responsable de l'audit interne.
   c. Le responsable de la conformité.
   d. Le management et l'ensemble du personnel dans toute l'organisation.

5. Parmi les critères suivants, lequel n'est pas pris en compte dans l'évaluation du risque inhérent ?
   a. Vulnérabilité.
   b. Probabilité.
   c. Impact.
   d. Soudaineté

6. Parmi les propositions suivantes, laquelle constitue le meilleur argument pour inciter le responsable de l'audit interne à tenir compte du plan stratégique de l'organisation lors de l'élaboration du plan d'audit interne annuel ?
   a. Insister sur l'importance de la fonction d'audit interne pour l'organisation.
   b. Veiller à ce que le plan d'audit interne soit validé par la direction générale.
   c. Formuler des recommandations visant à améliorer le plan stratégique.
   d. Veiller à ce que le plan d'audit interne favorise la réalisation des objectifs généraux de l'organisation.
7. Lorsque la direction générale accepte un niveau de risque résiduel que le responsable de l'audit interne juge inacceptable pour l'organisation, le responsable de l'audit interne doit :
   a. Faire immédiatement état du niveau de risque inacceptable au président du comité d'audit et au cabinet d'audit extérieur indépendant.
   b. Démissionner.
   c. En discuter avec les membres de la direction qui sont bien informés et, si la question n'est pas tranchée, la soumettre au comité d'audit.
   d. Accepter la position de la direction générale, car c'est elle qui définit l'appétence pour le risque de l'organisation.

8. Dans le cadre de la mise en œuvre du dispositif de management des risques d'une organisation, on demande au responsable de l'audit interne de diriger l'évaluation des risques de l'organisation. Parmi les situations suivantes, lesquelles ne seraient pas pertinentes pour protéger l'indépendance et l'objectivité de l'audit interne ?
    a. Une partie de la direction participe à l'évaluation de la probabilité et de l'impact de chaque risque.
    b. Les propriétaires des risques reçoivent une responsabilité pour chaque risque important.
    c. Un membre de la direction générale présente les résultats de l'évaluation des risques au Conseil et précise qu'ils représentent le profil de risque de l'organisation.
    d. La fonction d'audit interne obtient l'aide d'un consultant externe pour mener à bien la session d'évaluation formelle des risques.

9. Une mission d'audit interne a été définie dans le cadre du plan d'audit interne annuel. D'après le modèle de risque de la fonction d'audit interne, cet audit est considéré comme étant à risque modéré. Le cycle d'audit en cours s'étend sur deux ans. Parmi les situations suivantes, laquelle aura certainement l'impact le plus fort sur la planification de la mission et sa durée pour cette mission d'audit interne ?
    a. Le domaine audité requiert le traitement d'un volume important de transactions.
    b. Certaines composantes du processus sont externalisées.
    c. Un nouveau système a été mis en œuvre en cours d'année et a changé le mode de traitement des transactions.
    d. Les montants traités ne sont pas négligeables.

10. La crise financière chez les PTFs qui réduit significativement les ressources d'un Etat est liée le plus directement à quelle catégorie d'objectifs ?
    a. Objectifs stratégiques.
    b. Objectifs opérationnels.
    c. Objectifs de reporting.
    d. Objectifs de conformité.

METHODOLOGIE ET OUTILS D'ELABORATION DE LA CARTOGRAPHIE, DU PLAN DE MITIGATION ET DU PLAN D'AUDIT BASES SUR LES RISQUES	**Date :**	**Durée**
Séquence 2 : Comment élaborer une cartographie ou registre des risques ?	**Classement : Sq2**	**Rédacteur : SS**
Objectifs	♦ Maîtriser la démarche et les outils d'élaboration d'une cartographie des risques ♦ Maîtriser les techniques d'identification et d'évaluation des risques ; ♦ Maîtriser les grilles d'analyse des risques	

Déroulement

N° Fiches	Titres / Contenu	Stratégie d'animation
5	La cartographie des risques : objectifs et démarche	Exposés, discussions
6	Comprendre les processus	Exposés, discussions
7	Identification et description des «ensembles homogènes » : l'univers d'audit	Exposés, discussions
8	Identification et évaluation des risques bruts ou inhérents	Illustrations
9	Identification et évaluation du contrôle interne	Illustrations
10	Evaluation des risques résiduels	Illustrations
Test de connaissances	**QCM synthèse risques**	Travaux de groupe de 5 (durée 1 heure 30)
Cas pratique	Cas pratique : Elaboration de la cartographie, du plan de mitigation et du plan d'audit basé sur les risques	Travaux de groupe de 5 (durée 2 heures)

FICHE N°5 La cartographie des risques : objectifs et démarche

1. Normes professionnelles, modalités pratiques d'application et prises de position pertinentes IIA

2010 —Planification
2120 — Management des risques
2200 — Planification de la mission

Modalité pratique d'application 2010-1 :	Prise en compte des risques et des **menaces** pour l'élaboration du plan d'audit
Modalité pratique d'application 2120-1 :	Évaluer la pertinence des processus **de** management des risques
Modalité pratique d'application 2200-1 :	Planification de la mission
Modalité pratique d'application 2210-1 :	Objectifs de la mission
Modalité pratique d'application 2210.A1-1 :	Évaluation des risques dans la planification de la mission

2. La cartographie des risques : définition

La cartographie des risques est un document qui permet de recenser et d'évaluer les risques majeurs d'une organisation et de les présenter de façon synthétique sous une forme hiérarchisée pour assurer une démarche globale de maîtrise de ces risques.

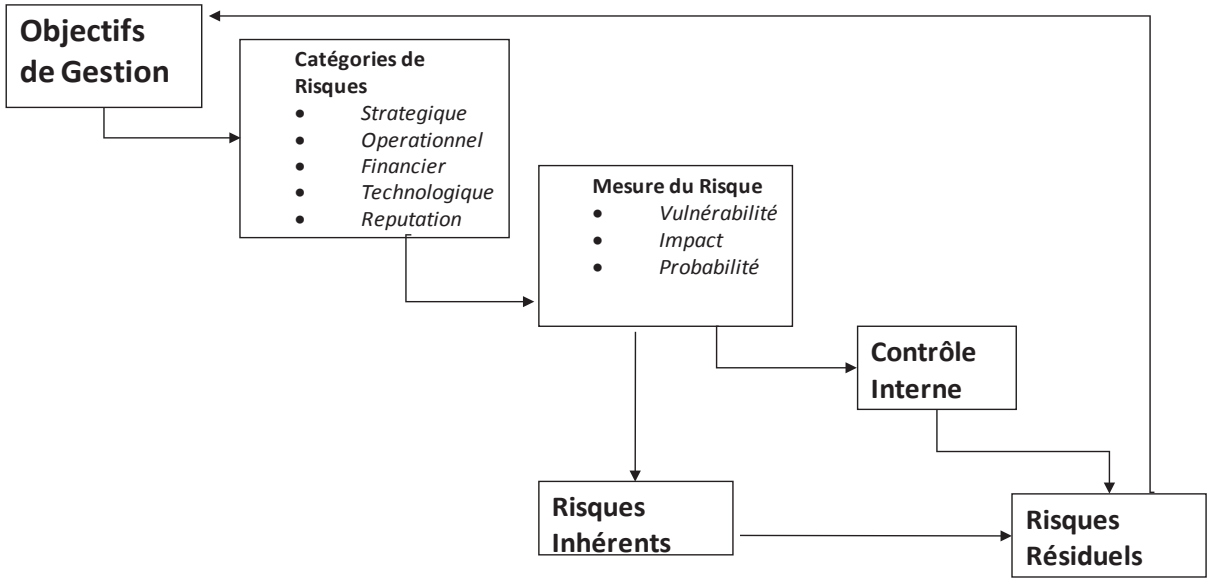
Cette hiérarchisation s'appuie sur les critères suivants :
- L'impact potentiel
- La probabilité de survenance
- Le niveau actuel de maitrise de risques

3. La cartographie des risques : objectifs et utilités

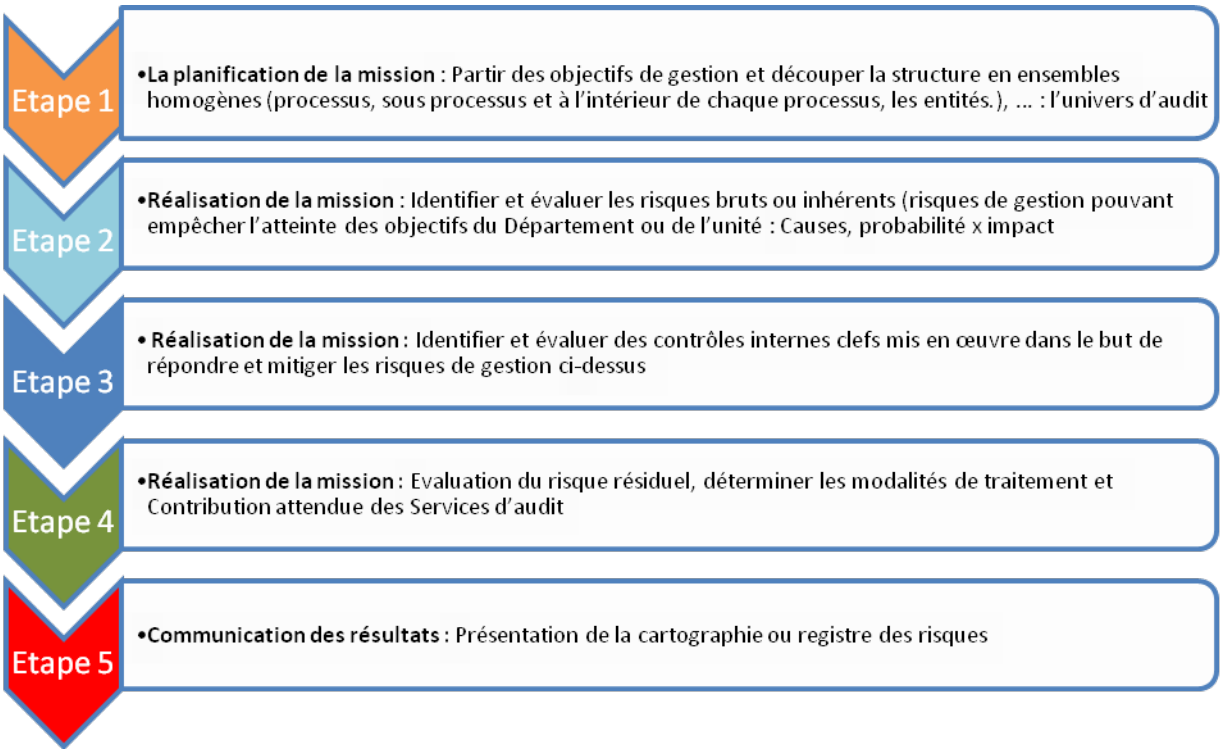
L'établissement d'une cartographie des risques peut être motivé par les objectifs suivants :

- Mettre en place un contrôle interne ou un processus de management stratégique et opérationnel des risques en fonction des ressources disponibles;
- L'allocation stratégique des ressources (humaines, matérielles, financières, etc.), en fonction de la qualité du dispositif de maîtrise des risques prioritaires ;
- Mettre en place une stratégie de communication interne et externe relative à la gestion des risques ;
- Assurer le suivi du plan d'action ;
- Aider le management dans l'élaboration de son plan stratégique et de sa prise de décision ;
- Orienter le plan d'audit interne (pluriannuel et annuel, et individuel des missions) en mettant en lumière les processus au niveau desquels se concentrent les risques majeurs ;
- Renforcer la bonne image de l'organisation ;
- Référentiel d'analyse permettant de choisir la démarche à adopter en matière de gestion des risques.

4. La cartographie des risques : étapes de réalisation



-
-



5. Planification de la mission

Le processus de planification doit porter sur la définition des objectifs et du périmètre, le calendrier de la mission, les prévisions d'effectifs et les budgets financiers.

La planification de la mission d'élaboration de la cartographie des risques conduite par l'audit interne doit également permettre de connaitre l'audité, notamment ses objectifs et ses assertions.

5.1 La connaissance de l'audité et ses assertions

Pour mener la mission de cartographie des risques et d'élaboration du plan d'audit basé sur le risque avec efficacité[6], l'auditeur doit en premier lieu comprendre les objectifs de l'audité, les tâches effectuées dans le domaine examiné qui visent à atteindre ces objectifs, ainsi que les mécanismes de pilotage des performances et de mesure de la réussite.

La simple prise de connaissance des processus dans de l'entité n'est pas suffisante et présente des risques quant à la qualité de l'interprétation qui en est faite. Il convient, pour avoir une information fiable, de se référer aux documents sources, rassemblés *dans un dossier unique pour toutes les entités*.

La constitution du **dossier de référence** (dossier permanent) **peut passer par l'obtention des informations de base ci – après (Réf. 5 Kit) :**

- la définition de la mission de l'entité, les objectifs et les plans (missions, objectifs stratégiques, opérationnels, indicateurs de performance) ;
- des informations sur l'organisation par exemple, l'organigramme général et détaillé, les descriptions de poste le nombre et les noms des collaborateurs, les collaborateurs occupant des postes-clé, les manuels de procédure et de politique, ainsi que des détails sur les derniers changements d'organisation, y compris les changements importants de systèmes informatiques ;
- des informations budgétaires, des résultats des opérations, et des données financières sur l'activité à auditer ;
- les dossiers d'audits précédents ;
- des résultats d'autres audits, y compris ceux des auditeurs externes, terminés ou en cours ;
- des dossiers pour déterminer des problèmes potentiels importants ;
- la littérature technique faisant autorité pour l'activité.

La constitution de ces dossiers nécessite des relations préliminaires avec l'audité, notamment, les différents services de doctrine ou d'élaboration des directives, normes internes et procédures. Il est en particulier essentiel d'obtenir la ***validation des dossiers par les Directeurs opérationnels concernés afin d'être certains de la référence qu'utiliseront les auditeurs***.

La constitution de ces dossiers est un moment important de la démarche d'élaboration de la cartographie et du plan d'audit basé sur les risques, elle permet la formalisation **de la lettre de mission (Lettre de mission Réf. 1 Kit).**

Un atelier d'échange et de cadrage avec tous les acteurs impliqués (managers, opérationnels) peut être organisé pour permettre aux participants de :

- comprendre et s'accorder sur les concepts, les techniques et les outils ;
- Comprendre comment les organisations structurent leurs activités pour atteindre leurs objectifs ;
- appréhender les différents rôles attribués aux managers et à l'audit interne dans le management des risques dans une organisation ;
- comment identifier les processus clés d'une organisation ;
- Maîtriser le concept processus et savoir le documenter ;
- Comprendre les risques de base auxquels sont confrontées les organisations ;
- Identifier et évaluer les principaux risques (majeurs) pesant sur la réalisation des objectifs de l'organisation et leur relation avec les processus ;
- Savoir élaborer un univers d'audit pour une organisation, proposer après évaluation des risques résiduels, un plan de mitigation.

[6] Ou de mise à jour de ces outils

5.2 Déterminer les objectifs et le périmètre de la mission : la lettre de mission

La mission d'élaboration ou l'actualisation de la cartographie des risques conduite par l'audit interne ***entre la catégorie des missions mixtes d'assurance et de conseil*** qui vise la palette d'objectifs suivants :

- l'évaluation indépendante d'un processus ou de contrôles.
- des conseils aux managers à tous les niveaux de l'organisation sur la manière de documenter et de regrouper leurs évaluations des risques et des contrôles.
- Faciliter les autoévaluations :
    - l'évaluation par la direction générale des risques qui menacent l'organisation dans son ensemble;
    - l'évaluation par les propriétaires des processus des risques qui menacent leurs activités.
- Mener des formations en interne :
    - renseigner les audités et leur hiérarchie sur les nouvelles lignes directrices qui font autorité sur la gouvernance d'entreprise, le management des risques et le contrôle ;
    - informer les propriétaires des processus et le personnel sur les concepts fondamentaux que sont la gouvernance d'entreprise, le management des risques et le contrôle.

La lettre de lancement de la mission doit, notamment préciser (Lettre de mission Réf. 1 Kit) :

- l'objet de la mission
- en pièces jointes :
    - le planning de réalisation de la mission (macro programme : Réf. 02 Kit)
    - la liste de la documentation nécessaire et des personnes à rencontrer (Liste documentation nécessaire et personnes à rencontrer, Réf. 5 Kit)
- le type de mission : Mixte
- Le directeur de mission :
- Destinataires : responsables des entités auditées
- Copie pour information : toute personne impliquée ou concernée

1. Origine et justification de la mission
2. Résultats attendus (y compris, la forme et le contenu de la cartographie qui varient naturellement d'une organisation à une autre en fonction des choix et des finalités recherchées)
3. Les méthodes d'identification et d'évaluation des risques à mettre en œuvre (Approche qui est participative : application de la méthode MIRIS)
4. Périmètre et limites
    a. Géographique
    b. fonctionnelle

5. Responsabilité de la mission (composition de l'équipe)
    - Chef de mission : …….
    - Auditeurs :
    - Le contrôle qualité (éventuellement).
6. Calendrier de la mission (date de début et durée prévisionnelle)
7. Les moyens à mettre à la disposition des auditeurs (personnel, véhicules, accès aux outils informatiques).

La lettre de mission (un original) signée sera retournée par l'audité avec la mention « Bon pour accord».

Nota : à propos des limites (périmètre de la mission)

La lettre de mission définit le périmètre de chaque cartographie des risques suivant les besoins et les objectifs poursuivis :

- toute l'organisation (cartographie globale), une unité de gestion (business unit), un site (cartographie sectorielle ou thématique), ou uniquement un projet pilote;
- tous les objectifs ou les objectifs clés ;

- tous types de risques ou des risques spécifiques.

5.3 Élaborer un programme de travail et allouer des ressources

Une planification détaillée avec affectation des ressources est faite. Un **programme de travail formel** présente les principales activités du processus de la mission et tout jugement formulé concernant les objectifs et le périmètre de la mission **(Planning de travail, Réf. 3 Kit).**

En se fondant sur les activités à réaliser au cours de la mission, l'auditeur doit identifier et désigner les membres du personnel correspondant au niveau d'expérience et de compétence approprié, afin que la mission puisse être menée dans les temps et avec efficacité.

Il y a lieu également d'estimer les **moyens logistiques et financiers** nécessaires à la correcte réalisation de la mission **(Budget type ABR, Réf. 4 Kit)**:

- Bureau
- Équipements
- Fournitures de bureaux
- Déplacement
- Prise en charges des auditeurs
- Etc.

5.4 La réunion d'ouverture

Fortement recommandée, conduite par le chef de mission, elle réunit la hiérarchie supérieure et les opérationnels de la structure « auditée[7] » (futurs interlocuteurs) et a pour objectif de préciser avec ces derniers :

- l'objet de la mission,
- les attentes prioritaires des audités,
- le cadre et les limites,
- la date de début et la durée prévisionnelle,
- le ou les structures concernées,
- la composition de l'équipe d'audit,
- l'approche et les outils,
- l'ordre de passage (**Fiche de prise de rendez – vous, Réf. 8 Kit),**
- si cela est nécessaire, les moyens à mettre à la disposition des auditeurs (personnel, véhicules, accès aux outils informatiques).

La réunion d'ouverture est sanctionnée par un procès-verbal **(PV réunion d'ouverture, Réf. 8.1 Kit).**

Le travail terrain peut alors commencer !!!.

[7] Entité dont la cartographie des risques est envisagée (élaboration ou actualisation)

FICHE N°6 Comprendre les processus

1. Les processus : définition

Les organisations structurent leurs activités pour mettre en œuvre leur stratégie et atteindre leurs objectifs (organisationnels). Les ***activités sont structurées en processus ou en projets***. Au sein d'une même organisation, les Processus peuvent différer fortement entre les secteurs d'activité.

Qu'est-ce qu'un processus ? C'est *simplement* ***l'ensemble des activités reliées les unes aux autres qui permet d'atteindre un objectif un but*** (résultats).

Un processus est ***un ensemble d'activités corrélées ou interactives qui transforment les éléments d'entrée en éléments de sortie (norme ISO 9001:2000).***

Un exemple pour illustrer :

Prenons un objectif simple : arriver à l'heure au cours à 8h00 demain matin. Détaillons maintenant les étapes conduisant à cet objectif : Vous pouvez :

1. mettre dans votre sac le cahier du participant et tout ce dont vous aurez besoin, ainsi que votre ordinateur portable ;
2. mettre votre réveil à sonner pour 6h00, et aller vous coucher
3. vous lever quand votre réveil sonne ;
4. Vous doucher
5. vous habiller ;
6. prendre votre petit déjeuner ;
7. Prendre votre voiture
8. Conduire jusqu'à la salle
9. Vous garer
10. marcher jusqu'à la salle de formation ;
11. choisir sa place ;
12. prendre place.

Pour élaborer cette liste, vous avez procédé à un certain nombre de choix, parmi différentes options que vous auriez pu prendre. Ainsi, vous auriez pu préparer votre sac le matin au lieu du soir.

Pourquoi avez-vous fait ces choix ?
Dans certains cas, il peut s'agir de préférences personnelles. Ainsi, si vous faites votre sac la veille, vous pouvez dormir cinq minutes de plus le lendemain matin. Dans d'autres cas, votre choix peut avoir une incidence directe sur votre capacité à atteindre votre objectif.

Ainsi, vous avez décidé de régler votre réveil au lieu de vous fier à votre horloge intérieur pour vous réveiller à 6H00. Dans ce cas, vous tenez le raisonnement sur le management des risques.

Les organisations recourent au même processus de réflexion pour planifier les étapes qui les aideront à atteindre leurs objectifs, c'est à dire l'identification des risques potentiels pesant sur ces objectifs et le management de ces risques pour les ramener à des niveaux acceptables.

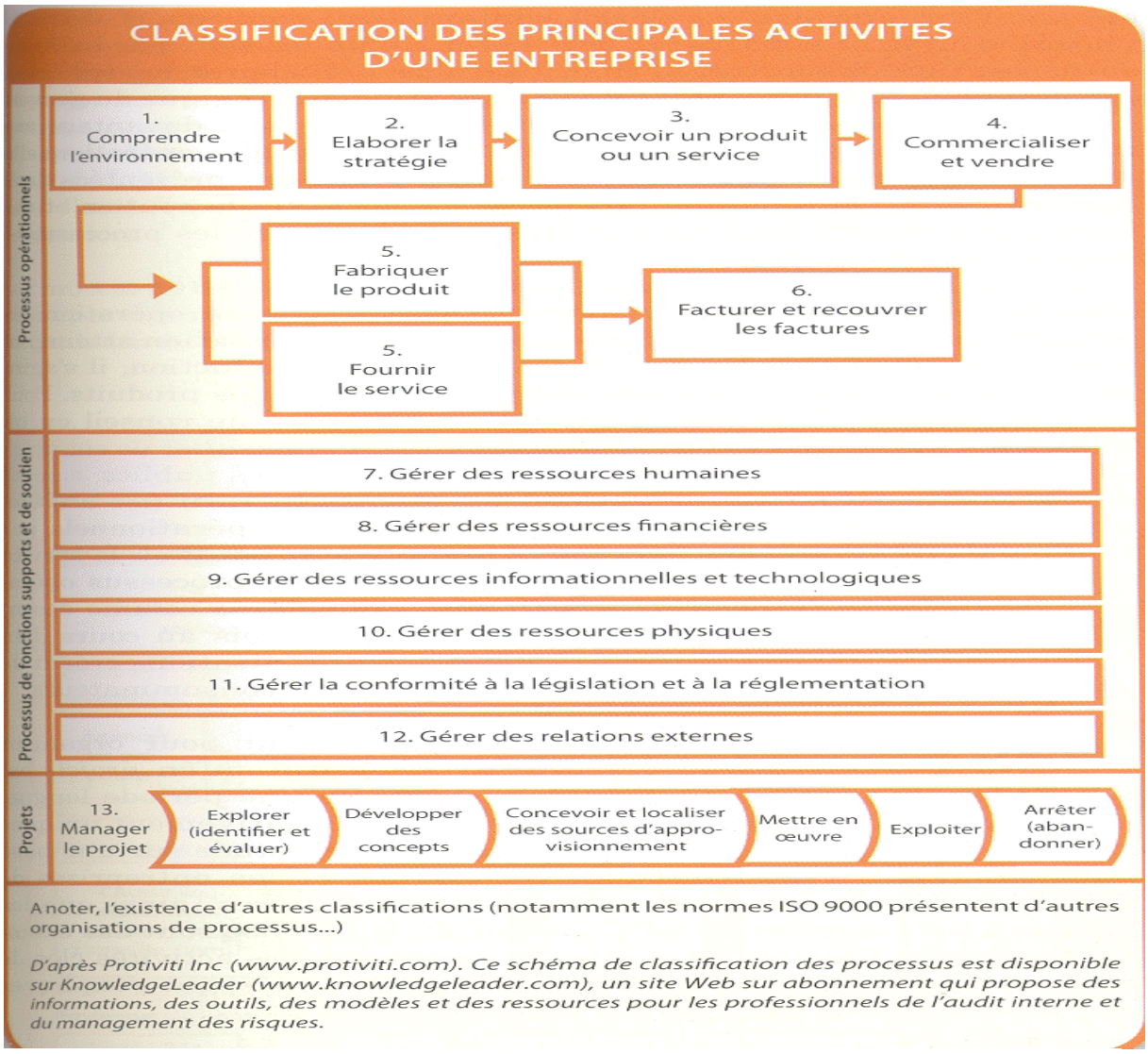
Dans toute organisation, il peut être identifié 3 types de processus :

- les processus opérationnels (de pilotage[8] et de réalisation ou de métiers)
- les processus de gestion et de soutien (fonctions supports),

[8]de management ou décisionnels

- ainsi que les projets.

L'encadré ci-dessous présente une ***classification de base pour les entreprises***.



Les processus opérationnels représentent l'activité cœur de métier[9] de l'organisation :

- de l'élaboration à la prise de commande,
- la livraison des produits et services pour les clients.

Pour une entreprise de production, il s'agit des processus par lesquels elle fabrique et vend des produits. Pour les prestataires de services, comme un cabinet de conseil ou un établissement financier, ce sera le processus par lequel ils commercialisent et fournissent leurs services.

Les services publics ou les organisations à but non lucratif (les associations... par exemple) ont aussi **des processus opérationnels lesquels ils délivrent des services.**

Les processus de pilotage représentent l'activité d'élaboration des informations internes permettant le pilotage de l'activité de l'organisation.

[9]Processus clés grâce auxquels l'organisation atteint ses objectifs prioritaires

On distingue souvent :

- le pilotage opérationnel
- et le pilotage stratégique.

Les processus de support représentent l'activité de mise à disposition en interne des ressources nécessaires à la réalisation des processus opérationnels (à la création de la valeur):

- Achats de fournitures,
- RH (recrutement, gestion des carrières, formation, paie, etc.),
- Comptabilité, reporting, finances et trésorerie,
- Système d'information et communicationnel,
- etc.

Certaines organisations procèdent différemment pour organiser les activités créatrices de valeur. **La structuration en projets** utilisée lorsque les activités se déroulent sur *une période longue*. Le mode « projet » est aussi, souvent, utilisé par la plupart des organisations pour organiser ainsi des activités non routinières.

CARTOGRAPHIE DES PROCESSUS D'UNE STRUCTURE D'AUDIT

1. Processus opérationnels (gouvernance et métiers)

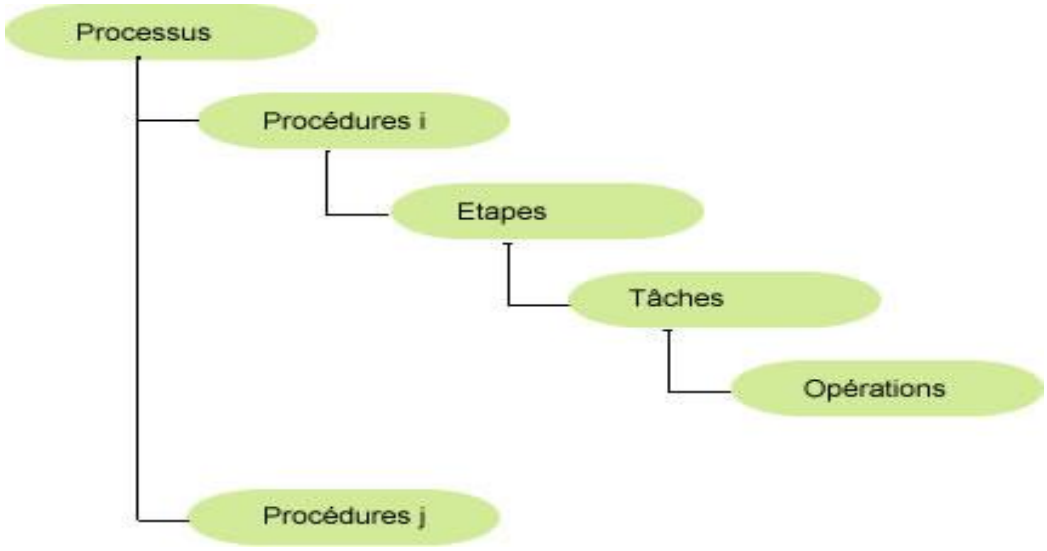
a) Comprendre l'environnement (interne et externe)
b) Comprendre les missions et les objectifs de gestion
c) Identifier et évaluer les risques liés aux différents objectifs de gestion
d) Elaborer un plan pluri annuel d'audit et programme annuel d'audit basés sur le risque
e) Réaliser des missions d'audit internes
f) Constituer des dossiers d'audit internes
g) Suivre les recommandations

2. Processus supports ou d'appui (soutien)

a) Gestion des ressources humaines
b) Gestion des finances et de la comptabilité
c) Gestion de l'administration et de la logistique (immobilisations et stocks)
d) Gestion de la conformité à la règlementation et aux prescriptions déontologiques
e) Gestion de la documentation, du système d'informationnel et de la technologique
f) Gestion des relations externe

2. Composition des processus

Chaque processus peut être décomposé en sous-processus (procédures) ou en phases (ou étapes) et chaque étape se compose de tâches et en opérations.



Le niveau de détail utilisé pour décrire ces processus variera selon le niveau de documentation souhaité (on peut aller des Macro-processus, aux processus, aux sous processus, aux activités, aux tâches et aux opérations).

Nota :

Il ne faut pas confondre **« processus » avec « procédure ».** Le premier décrit les activités de l'organisation selon une **vision transversale** par rapport à l'organisation de celle-ci tandis que le second **explicite le "comment faire" dans cette organisation**.

L'approche processus permet d'identifier et de maîtriser les interfaces entre les différentes activités.

- Le processus répond aux questions : QUOI FAIRE ? POUR QUELLE VALEUR AJOUTÉE ? QUI ?
- La procédure répond aux questions : COMMENT FAIRE ? QUAND ?
- Le mode opératoire répond de plus aux questions : OÙ ? SELON QUEL PROCÉDÉ ?
- Le mode pilotage répond de plus à la question : COMBIEN ?

L'utilisation d'une approche processus peut conduire à é*laborer une cartographie des processus* qui permet de représenter l'organisation à travers les liens entre les différents processus (voir classification de base ci-avant).

Un processus est caractérisé par 6 paramètres :

1. Le pilote (celui qui rend compte du fonctionnement du processus),
2. Les ressources requises (financière, humaine, matérielle...),
3. Les éléments d'entrée (données ou produits),
4. La valeur ajoutée,
5. Les éléments de sortie (données ou produits), et
6. Le système de mesure, de surveillance ou de contrôle associé.

Le processus peut être défini **dans une *fiche de données processus*** (« data sheet » en anglais) qui pourra **documenter les caractéristiques du processus** et apporter un complément d'information nécessaire à une compréhension la plus complète possible du fonctionnement du processus y compris, lorsque nécessaire, les objectifs à atteindre.

Dans le cas de processus complexe il pourra être adjoint une représentation graphique ainsi qu'une cartographie complète des processus[10].

[10] Voir R6 Cartographie des processus

Exemple de points à documenter dans une fiche de données processus :

- Les éléments d'entrée,
- Les éléments de sortie,
- Une description succincte du processus,
- La désignation du pilote, des acteurs, des supports et principaux moyens,
- Le ou les clients du processus,
- Le ou les fournisseurs du processus,
- Les points de mesure,
- Les moyens de surveillance,
- Les objectifs...

3. Les préalables : Comprendre, identifier, décrire et documenter les processus clés

Les auditeurs internes créent ou préserve de la valeur et améliorent les opérations d'une organisation, **en comprenant d'abord le modèle économique de celle-ci**. Ce modèle **énonce les missions et les objectifs de l'organisation et la manière** dont ses processus sont structurés pour atteindre ces objectifs.

3.1 Identification des processus clés

La première, descendante (top down[11]), part de l'organisation, avec ses objectifs, *puis identifie les processus clés critiques pour les atteindre*.

Un *processus est considéré comme clé par rapport à un objectif spécifique si sa défaillance aura pour conséquence directe d'empêcher l'atteinte de cet objectif*. Il est important de noter que si des processus ne sont pas clés pour un objectif spécifique, ils peuvent l'être pour un autre.

Remarque
Il est fortement recommandé d'envisager (dans les grandes structures notamment) une description détaillée et une modélisation exhaustives de tous les processus. Il convient donc de concentrer les efforts sur les processus clés à forte valeur ajoutée (agrégeant plusieurs métiers).

Une fois que les processus clés sont identifiés par l'équipe, ils sont analysés, détaillés et documentés. Chaque processus est scindé en **sous-processus**, jusqu'au niveau des activités.

Exemple : Processus de gestion des ressources humaines dans l'administration (décomposition du processus en sous processus)

- 1. expression des besoins
- 2. recrutement
- 3. formation
- 4. titularisation
- 5. système d'évaluation des fonctionnaires
- 6. formation
- 7. système de gestion des carrières
- 8. système de gestion des temps

[11] *Dans cette démarche ascendante, c'est l'équipe qui détecte les risques et les soumet pour avis aux opérationnels*

Exemple : Processus d'une structure d'audit

PROCESSUS	SOUS PROCESSUS	PROCEDURES/ ACTIVITES / TACHES
ASSURER LES AUDITS	Produire un plan triennal d'audit et programme annuel d'audit	Elaborer et mettre en œuvre le plan triennal d'audit et programme annuel d'audit
	Réaliser des missions d'audit internes	Exécuter les missions d'audit internes • Planifier ○ Déterminer les objectifs et le périmètre de la mission ○ Connaitre l'audité (ses objectifs et ses assertions) ○ Identifier et évaluer les risques ○ Identifier les contrôles clés existants ○ Evaluer l'adéquation de la conception des contrôles ○ Elaborer un plan de tests (programme de travail) ○ Allouer des ressources à la mission ○ Documenter et superviser • Conduire la mission ○ Réaliser les tests pour collecter des preuves ○ Evaluer les preuves rassemblées et en tirer des conclusions ○ Faire des observations et formuler des recommandations ○ Documenter et superviser ○ • Communiquer les résultats ○ Evaluer les observations et faire remonter l'information ○ Procéder à des communications préliminaires et intermédiaires (rapport provisoires) ○ Rédiger le rapport d'audit final ○ Procéder aux communications informelles et formelles des résultats définitifs
	Constituer des dossiers d'audit internes	Classement des dossiers d'audit
	Suivre les recommandations	Mettre en œuvre des procédures de surveillance et de suivi

Cette approche est efficace car **elle produit un ensemble gérable de processus critiques**. Elle est généralement adoptée par une équipe possédant **une vaste vue d'ensemble de l'organisation**, mais sans connaissance détaillée de chaque domaine. Cependant, elle peut conduire à négliger des processus qui se révèlent in fine critiques[12].

[12] Valider l'identification des processus clés avec les propriétaires des processus.

L'approche ascendante (bottom up[13]) commence par une revue de tous les processus au niveau des activités par les opérationnels. Elle nécessite donc que tous les services de l'organisation identifient et documentent les processus auxquels ils participent.

Cette tâche est exécutée par les personnes responsables des activités en question. Les processus identifiés sont ensuite agrégés sur l'ensemble de l'organisation. Si cette approche fonctionne bien pour des organisations *de petite taille comportant un nombre limité de processus*, **elle est moins efficace pour les organisations grandes et complexes (comme les Ministères) car il devient difficile de classer, par ordre de priorité, l'importance de chaque processus par rapport aux autres.**

3.2 Détermination des objectifs clés (arborescence)

Une fois un processus identifié, l'étape suivante, quelle que soit l'approche, consiste à déterminer ses objectifs clés (voir **fiche de données processus ci-dessus)**. Il faut alors répondre aux questions suivantes :

- Pour un auditeur interne, ou quelqu'un qui ne participe pas directement au processus, la première source d'information **est :**
  - **le propriétaire du processus**
  - **et la documentation existante sur les politiques**
  - et les procédures dudit processus.

Dans l'idéal, son propriétaire a défini des objectifs formels qui répondent aux questions ci-dessus (voir **fiche de données processus ci-dessus**). Sinon, l'auditeur interne devra, pour obtenir ces informations nécessaires, travailler avec les personnes impliquées dans ce processus (les propriétaires des risques).
Une fois les objectifs du processus compris, il s'agit d'analyser les données d'entrée et les activités spécifiques nécessaires pour parvenir aux objectifs et aux résultats du processus.

- Pour comprendre comment ces données et activités se combinent pour générer de résultats, il convient de commencer par analyser les documents existants, par exemple :

- Dossier permanent (s'il existe) ;
- Les textes fondateurs ;
- L'organigramme ;
- manuels de procédures ;
- les politiques liées au processus ;
- description de postes des personnes concernées ;
- le diagramme de flux des processus.

Même si les documents existants constituent un point de départ, il est généralement nécessaire de discuter des différents aspects du processus avec les personnes qui en ont la responsabilité.

1. Pourquoi ce processus existe-t-il ?
2. Sur quels objectifs stratégiques de l'organisation le processus peut-il avoir une incidence et comment ?
3. « Quelles initiatives, actions, le processus doit-il déclencher pour aider l'organisation à atteindre ses objectifs stratégiques ?
4. Qu'apporte le processus à l'organisation, sans quoi elle aurait du mal à prospérer ?
5. En fin de compte, qu'est-ce qui donne aux salariés participant au processus un sentiment de satisfaction dans leur travail ?
6. Quelles sont les réalisations qui permettent aux salariés participant au processus d'être reconnus par la direction ou par les clients internes ?

[13]Dans cette démarche ascendante, ce sont les opérationnels qui identifient les risques. Ces risques sont ensuite soumis à l'équipe pour validation, analyse et évaluation.

7. Comment les individus concernés par le processus sont-ils censés agir et que se passe-t-il s'ils ne répondent pas à cette attente ?
8. Existe-t-il des indicateurs permettant de mesurer et de suivre les performances ?

Pour comprendre le processus, il faut non seulement identifier les objectifs clés, mais également comprendre comment la direction et le propriétaire du processus savent si celui-ci fonctionne comme prévu. Le propriétaire du processus doit avoir défini des indicateurs clés pour *suivre les performances du processus.*

- **Ces indicateurs doivent être :**
  1. Observables (ils peuvent être mesurés objectivement) :
  2. Pertinents pour l'objectif en question (et non pas utilisés simplement parce qu'ils peuvent être quantifiés) ;
  3. Rapidement disponibles ;
  4. Communiqués aux personnes concernées par le processus.

Les indicateurs clés de performance ou d'autres types d'indicateurs peuvent indiquer les attentes de la direction, ou son niveau de tolérance sur les résultats du processus.

Référentiel des indicateurs

Domaine ou objet auditable	Dimensions	Indicateurs	Mesures	Normes ou cibles de performance

Observations

Il est impératif de décrire par écrit le processus. Ce sont généralement *le propriétaire et les responsables du processus qui doivent s'en charger*.

Cependant, il peut arriver qu'ils ne le fassent pas à cause des impératifs quotidiens de leur travail ou parce qu'ils n'en voient pas l'utilité. Si l'absence de description a peu de conséquences immédiates, avec le temps et à mesure que les personnes concernées changent de poste ou quittent l'organisation, les *objectifs du processus risquent d'être perdus ou faussés*.

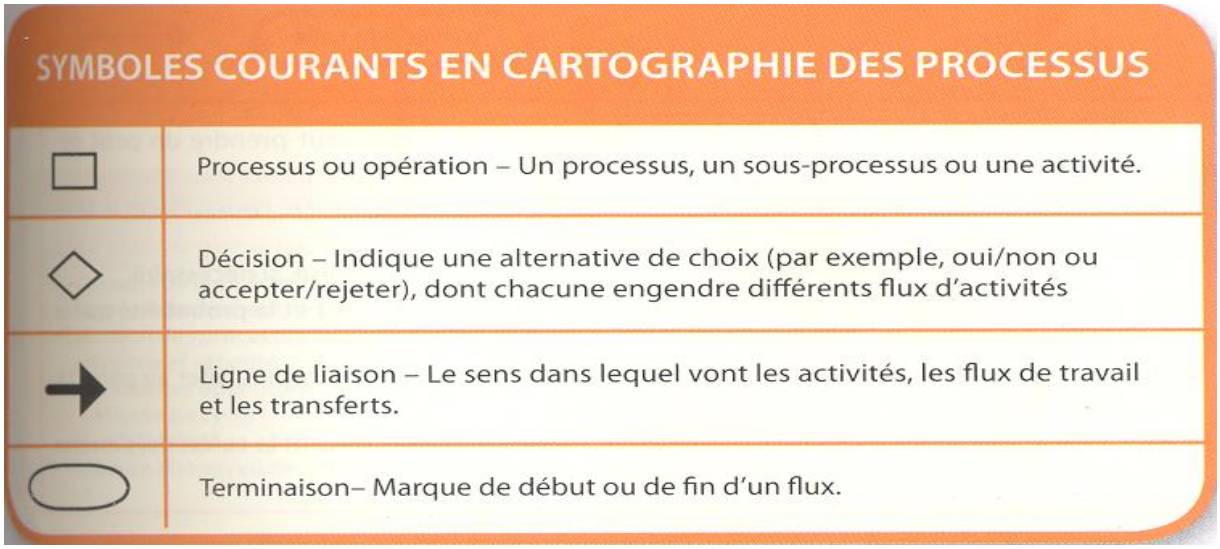
- La **description écrite du processus peut se révéler très efficace pour :**
  1. Orienter les nouveaux salariés,
  2. Définir les périmètres de responsabilité,
  3. Evaluer l'efficience des processus,
  4. Déterminer des zones prioritaires,
  5. Identifier les principaux risques et contrôles.

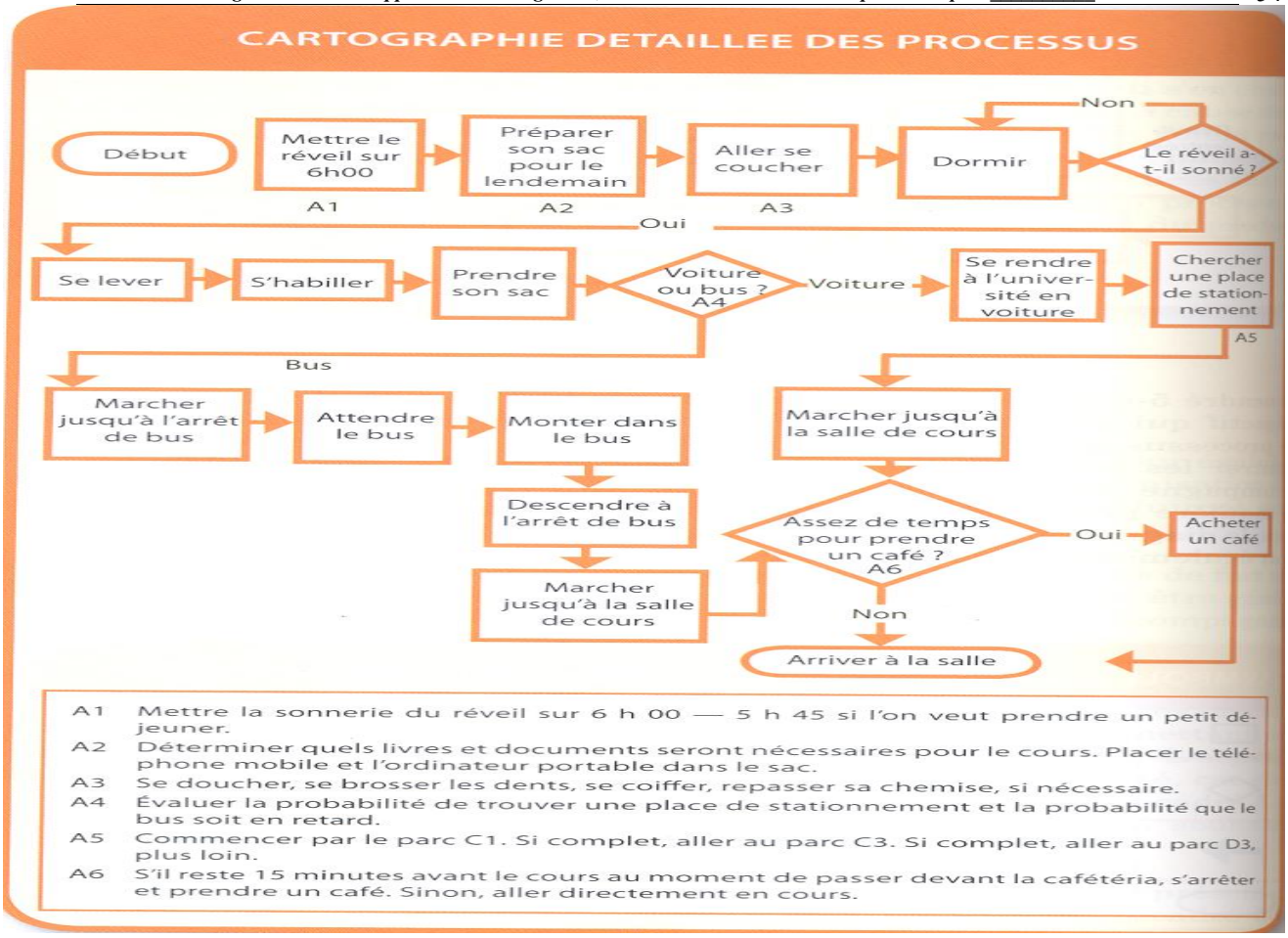
Les auditeurs internes doivent également ***documenter leur évaluation globale des risques*** et des contrôles au sein de l'organisation et dans toutes missions spécifiques d'assurance qu'ils conduiront sur le processus en question.

Deux outils sont généralement utilisés :

- les diagrammes de flux,
- et les descriptions narratives des processus.

Les diagrammes **peuvent être généraux ou détaillés** activité par activité. Ils peuvent s'accompagner d'un texte.





Modalités pratiques d'application

Voir Kit du cartographe, Réf 6 : Description de la cartographie des processus et Réf 10 : Fiche de description de poste.

FICHE N°7 — Identification et description des "ensembles homogènes" : l'univers d'audit

1. Position du problème : Les prescriptions de la norme IIA 2010 - Planification

Le responsable de l'audit interne doit établir **une planification fondée sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation**.

Interprétation :

Il incombe au responsable de l'audit interne de développer un plan d'audit fondé sur les risques. Pour ce faire, le responsable de l'audit interne prend en compte le système de management des risques défini au sein de l'organisation, il tient notamment compte de l'appétence pour le risque définie par le management pour les différentes activités ou branches de l'organisation. Si ce système de management des risques n'existe pas, le responsable de l'audit interne doit se baser sur sa propre analyse des risques après consultation des instances dirigeantes.

2010.A1 – Le plan d'audit interne doit s'appuyer sur une évaluation des risques **documentée et** réalisée **au moins une fois par an**. Les points de vue des instances dirigeantes doivent être **pris en compte dans ce processus**.

2010. C1 – Lorsqu'on lui propose une mission de conseil, le responsable de l'audit interne, avant de l'accepter, **devrait** considérer dans quelle mesure elle est susceptible de créer de la valeur ajoutée, d'améliorer le management des risques et le fonctionnement de l'organisation. Les missions de conseil qui ont été acceptées doivent être intégrées dans le plan d'audit.

Ainsi, planifier les activités de l'Audit Interne c'est élaborer un plan à partir d'une cartographie des risques, définir un planning et prévoir un système de reporting des résultats obtenus auprès de la hiérarchie concernée. Le plan d'Audit Interne peut comprendre un plan-pluriannuel et un programme annuel.

L'élaboration de la cartographie des risques ***est l'étape (l'outil) indispensable de l'identification institutionnelle des besoins d'audit (plan d'audit) d'une organisation.***

La réalisation d'une cartographie des risques dans une organisation permet de disposer d'une vision d'ensemble, exhaustive et précise, de son exposition aux risques (aux turbulences) de toutes natures, tant internes qu'externes.

Indépendamment du plan d'audit (missions d'audit) **qui en découlera** ultérieurement, la cartographie des risques (situation des risques auxquels l'organisation est exposée en considération de son dispositif de contrôle) permet **par ailleurs de définir (identifier) les dispositifs adéquats à mettre en place pour maitriser ces risques.**

➥Les quatre (4) étapes classiques à suivre pour l'élaboration d'une cartographie des risques sont :

1. Découper l'organisation en «ensembles homogènes »
2. Identification et évaluation des risques bruts ou inhérents
3. Identification et évaluation du contrôle interne
4. Evaluation des risques résiduels.

2. La démarche : L'univers d'audit en 3 tâches

Etape 1 : Identification et description des ensembles homogènes (métiers ou missions, entités, processus)

-**La première étape** consiste à découper l'organisation en ensembles homogènes (métiers, à l'intérieur de chaque métier, les entités et enfin au sein de chaque entité les différents processus : planification, achats, production, GRH, logistique, production, informatique, etc.) **(Tâche 1) : partir des missions ou objectifs**
Nota : En fonction du degré de précision souhaitée de cette cartographie des risques, ce découpage pourra évoluer d'un niveau très global « métiers », à un niveau intermédiaire « entités » à l'intérieur de chaque métier, ou encore à un niveau beaucoup plus détaillé « processus » de chaque entité à l'intérieur de chaque métier **(domaines, Missions, objectifs, activités, tâches : colonnes 1, 2 et 3 de la matrice).**

-Pour chaque ensemble homogène, obtenir une description (buts et objectifs de gestion poursuivis, moyens alloués, volume traités, … **(Tâche 2)** (Cartographie des processus, **Réf. 6 Kit** et Fiche de description de poste, **Réf. 10 Kit**), fiche de séparation des fonctions **(Non référencé dans Kit).**

Plusieurs sources d'informations sont utilisées pour réaliser cet inventaire : service contrôle interne, service risk management, opérationnels, …) : Liste de documentation nécessaire et personnes à rencontrer, **Réf. 5 Kit**

Cette étape **aboutit à une cartographie des ensembles homogènes ou univers d'audit (Tâche 3) :** Fiche de description des ensembles homogène – univers d'audit **- Réf. 7 et 7.1**.

⟹ **Livrables Etape 1 (tâches 3) :** **Cartographie des ensembles homogènes ou univers de management et d'audit**

3. Les approches possibles pour dresser l'univers d'audit

⧫⧫⧫ Le découpage de l'organisation en ensembles homogènes ou univers de management et d'audit peut être fait selon les différentes approches suivantes:

⧫*Approche par les métiers ou structure*

On découpe des sujets d'audit en fonction des grands métiers de l'entité : acheter, vendre, fabriquer, gérer, etc. A chaque métier correspond un ou plusieurs services : c'est aussi une approche par les structures. Il s'agit de partir de l'organigramme de l'entreprise dont chaque case doit être auditée ou du groupe.

⧫*Approche par les processus*

On part des processus (processus de gouvernance, processus métiers et processus supports, projets) :

- processus de production,
- processus des achats / ventes,
- processus de la trésorerie,
- Etc.

Cette approche permet d'analyser les activités de l'organisation de façon transversale en passant d'un service à l'autre, de regarder le fonctionnement des interfaces et l'efficacité des processus de contrôle interne. Elle permet de mieux apprécier le contrôle interne dans sa globalité.

Approche par les thèmes

Un thème ne correspond ni à un seul service ni à un seul cycle et sa nature permet d'aborder des missions d'audit spécifiques. On peut citer :

- audit des contrats,
- audit de la micro-informatique,
- audit de la sécurité, etc.

Cette approche peut permettre de déceler des faiblesses de contrôle interne concernant l'ensemble des services ou l'ensemble des cycles que les autres approches n'auraient pas permis de détecter.

Résumé

Tâches / Responsables

1 Le responsable de l'audit interne liste tous les ensembles potentiellement auditables sur la période du plan d'audit. Si l'organisation dispose d'une cartographie des risques, ces ensembles auditables peuvent correspondre à la notion « d'ensembles homogènes » définie précédemment. Ce listing se doit d'être exhaustif, pour cela plusieurs approches permettent de cerner les missions possibles :

- Approche par « métier » de l'organisation
- Approche par « entité » : filiales, usines, délégations régionales, agences…
- Approche processus : audit du processus « achats », du processus « gestion des stocks »…
- Ou encore approche thématique : audit de la sécurité, de la communication, de la politique de vente….

2 Les ensembles homogènes sont élaborés et validés avec les opérationnels (lors de l'atelier de cadrage).

Nota : La méthode utilisée est généralement la combinaison de ces différentes approches.

FICHE N°8 Identification et évaluation des risques bruts ou inhérents

1. Problématique de la gestion du risque

Les risques sont des événements incertains susceptibles d'affecter la réalisation des objectifs de l'organisation :

- *Impact négatif – non atteinte des objectifs*
- *Impact positif ou opportunité– événement apportant un bénéfice non attendu à l'organisation*

Si un événement est certain– ce n'est pas un risque

Les risques peuvent être mesurés en termes de:

- ***Vulnérabilité**: L'organisation est-elle susceptible d'être exposée à ce risque?*
- ***Probabilité:** Quelle est la probabilité que ce risque aura lieu et avec quelle fréquence?*
- ***Impact:** Quelle est l'ampleur, conséquence de cet événement?*

➟Les sinistres et les catastrophes se multiplient et avec elles les réactions se font de plus en plus fortes:

- *« Comment est-ce possible? »,*
- *« Comment a-t-on pu en arriver là ?»,*
- *« Pourquoi n'avoir pas réagi avant? »*

En effet, si la survenance d'incidents plus ou moins graves n'a rien de nouveau et si la prévention et la réactivité étaient et demeurent des saines pratiques reconnues, on note bien qu'aujourd'hui le manque de vigilance, d'anticipation et de sens des responsabilités est nettement moins bien accepté.

L'aléa n'est plus une donnée incontournable ... plus une justification en soi.

Les marchés financiers pour ce qui est des investissements, mais également **le public pour les causes nationales** (les catastrophes : inondations, tremblements de terre) ne pardonnent plus les erreurs de jugement et jugent plus sévèrement **ce qui relève de la force majeure** comme ce qui relève de ce qui aurait dû être géré.

On recherche et on valorise une certaine continuité, une sécurité accrue. Actionnaire, dirigeant, cadre, employé, fournisseur ou client, citoyens, nous sommes tous peu ou prou dans cette mouvance et nous recherchons une meilleure maîtrise de notre environnement, une sécurisation renforcée et une visibilité.

Les autorités de tutelle des secteurs sensibles (banque, assurance, santé, aviation ...) :

- *développent des **systèmes de normalisation**, de mesure, **de contrôle des risques** (réglementations prudentielles) ;*

- *et modulent agrément et marges de manœuvre en fonction des capacités de gestion des risques de chacun.*

Enfin, la bonne maîtrise de ses activités, **ce qu'on appelle le professionnalisme**, c'est-à-dire finalement **un niveau supérieur de savoir-faire technique n'est-ce pas d'atteindre avec plus d'assurance le meilleur niveau de performance en déjouant les pièges classiques et « se jouant" des imprévus et « coups du sort " ?**

Assurer sa performance, gérer les risques, mettre sous contrôle son activité ou une activité déléguée c'est bien évidemment fixer des objectifs, organiser des moyens et manager la performance **... mais c'est aussi faire face aux risques.**

➥ ***De quels risques parle-t-on ? On peut en distinguer 2 sortes :***

- ***Les risques d'activité ou risques métiers***[14]*, ceux qui pèsent sur tous nos projets comme ceux qui sont spécifiques à tel ou tel métier (sanitaire pour l'alimentaire, accidentel pour la distribution de carburant, de crédit pour la banque ...)*
- ***Les risques opérationnels****, ceux qui proviennent de l'organisation retenue, de notre capacité à la mettre en œuvre dans de bonnes conditions ... de nous tromper dans la mise en œuvre du bon dispositif (contrôle interne).*

Outre les différences intrinsèques évidentes, cette distinction est retenue pour **faciliter l'inventaire et la sélection des risques « à combattre"** dans un premier temps et pour préparer à des modes de gestion adaptés à chacune des catégories.

L'idée de départ est que quelle que soit l'organisation retenue, une entité est exposée à des risques d'une certaine nature et d'une certaine intensité appelés **« *risques bruts ou inhérent »***

Face à ces risques, les entités conçoivent avec plus ou moins d'à propos et d'efficience des réponses prudentielles (limites d'activité), organisationnelles, de procédures et de systèmes pour réduire ces risques. On nomme ces réponses « *dispositif de contrôle interne ou dispositif de maîtrise des risques*» (DMR).In fine, suivant l'efficacité et la permanence du DMR, une part plus ou moins importante **des risques bruts ou inhérents sont « filtrés».**

Il subsiste alors des « risques nets ou résiduels» impactant l'entité. Ces impacts **sont nommés « *incidents*»**. Ils sont observables, plus ou moins rapidement.

2. Mise en œuvre de la démarche et des outils :

Etape 2 : Identification et évaluation des risques bruts ou inhérents

Il s'agit d'élaborer une matrice d'évaluation (Rapport type élaboration cartographie et plan d'ABR **Réf. 16 Kit)** suivant les étapes ci-après :

[14] Les risques auxquels une entité est exposée sont pour une part importante directement liés à l'activité exercée.

1. **Identifier les <u>risques associés à l'objectif, la mission, le domaine, l'activité ou la tâche</u> (Tâche 1).**Il s'agit des inhérents (risques internes et externes) par rapport aux objectifs de contrôle interne :
   - respect des lois et règlements :
     - Non-respect des lois, règlements, obligations contractuelles
     - Faible qualité du système de pilotage
     - Sanctions insuffisantes
   - optimisation des opérations : risques affectant l'efficience, efficacité, économie des services fournis (intrants, processus, produits, résultats, impact)
   - sécurité des actifs : éthique, Fraudes
   - qualité des informations : fiabilité de l'information, compte rendu

2. **Rattacher le risque identifié à une <u>typologie de risque (menu déroulant avec 15 catégories de risque : voir infra) :</u> (Tâche 2).**
3. **Effectuer une analyse causale par type de risque identifié en rapport avec les composants du contrôle interne (Matrice d'évaluation de la qualité du contrôle interne, Réf. 11 Kit) : (Tâche 3).**
4. **Identification des conséquences probables (objectif, financier, humain, image, usagers/client/partenaire : voir grille cotation impact) : Tâche 4**
5. **Identification des responsables (propriétaire, clients, fournisseurs, supports) : (Tâche 3)**
6. **Pour chaque ensemble homogène et pour chaque nature de risque, procéder à une cotation de l'impact et de l'occurrence (Tâche 5) : voir Matrice concepts clefs: grille cotation probabilité et impact**
7. **Formaliser les résultats dans une matrice des risques bruts ou inhérents (PxI) : Tâche 6.**
8. **Définir l'ensemble des Bonnes pratiques de Contrôle interne communément admises de maîtrise des risques qui devront exister : Tâche 7.**

⟹ Livrables Etape 2 (tâches 6) : **Matrice des risques bruts ou inhérents**

Etape 2.1 Identification des risques et élaboration d'une typologie des risques (identification des risques bruts)

<u>Comment identifier les Risques majeurs inhérents ou bruts dans le secteur public?</u>

⇨ Les différentes techniques d'identification des risques sont les suivantes :

1. **Identification basée sur les actifs créateurs de valeurs** (risques associés aux actifs intangibles).
2. **Identification basée sur l'atteinte des objectifs** (un risque peut empêcher l'atteinte des objectifs; ces derniers sont d'abord définis, avant de leur associer les menaces pesant sur eux).
3. **Identification basée sur les check-lists:** liste déjà préconçue qui énumère l'ensemble des risques possibles afin de voir si chaque risque concerne l'entité ou pas.
4. **Identification par analyse historique**: identification en se basant sur les risques opérationnels déjà survenus au sein de l'entité.
5. **Identification basée sur l'analyse de l'environnement** (menaces de l'environnement économique, technologique…).
6. **Identification par analyse des activités:** décomposition des processus en activités identification des risques associés (conséquences potentielles de la non/mauvaise exécution des tâches).

<u>Nota</u>

Dans le secteur public, les trois techniques combinées généralement utilisées sont :

- L'identification basée sur l'atteinte des objectifs
- l'identification par analyse des activités
- Et l'identification par analyse historique

<u>Important</u> : Il ne s'agit pas d'identifier tous les risques : mais les risques critiques.

⇨ Démarche

Commencez d'abord par réfléchir en citoyen et usager des services publics, utilisez vos compétences d'audit et de gestionnaire par la suite.

En tant que citoyen et usager des services publics, il se peut que vous connaissiez certains des risques susceptibles d'affecter les objectifs du secteur public.

⇨ Vous connaitrez aussi quels sont les risques par :

- Votre propre expérience
- Les médias
- Les régulateurs
- Les bailleurs de fonds
- Rumeurs (mais faites attention…)
- Vos collègues
- *Un questionnaire (voir modèle COSO proposé) et entretiens (préparer le guide d'entretien) : Méthode MIRIS*

Les risques à considérer sont ceux susceptibles d'affecter la réalisation des **objectifs de l'organisation. La connaissance des objectifs de l'organisation doit donc précéder l'évaluation des risques**.

⇨ Utiliser un modèle type COSO pour identifier et définir les objectifs de l'organisation:

- Rendre compte
- Conformité
- Opérations
- Protection des ressources

Exemple générique d'une Classification des Risques (Taxonomie) dans le secteur public

Source du Risque	Catégories de Risque	Description
Interne	Stratégique	Risques liés aux mauvais choix stratégiques, définition des objectifs à long et moyen terme, politiques et priorités sectorielles.
	Opérationnel	Risques liés à la mauvaise exécution des plans et choix stratégiques. Ces risques s'expriment dans le court terme et dans le cadre de la programmation et planification annuelle.
	Ressources Humaines	Risques liés aux ressources humaines. Ces risques peuvent avoir des effets sur le capital humain. Par exemple: • Intégrité et honnêteté • Recrutement (fraude) • Connaissances et compétences • Bien-être des employés • Relation avec les employés • Rétention, et • Santé et sécurité au travail
	Information (pour aide à la décision)	Risques liés à l'accès et partage des connaissances & qualité des informations de gestion (opérationnelles, financières) disponibles au sein de l'organisation. Par exemple: • Disponibilité de l'information (temps, exhaustivité) • Stabilité de l'information • Intégrité, fiabilité de l'information • Pertinence de l'information • Rétention, et Protection

Source du Risque	Catégories de Risque	Description
	Litiges	Risques de pertes causées par un litige. Par exemple: • Réclamation des employés, du public, des fournisseurs de services • Défaut d'exercer ses droits
	Perte/Vol d'Actifs	Risques de pertes ou vol d'actifs
	Risque d'approvisionnement	Risques liés aux approvisionnements. Par exemple: • Coûts et stratégies d'approvisionnement • Accès aux ressources • Gaspillage des ressources matérielles
	Niveau de service	Les organisations du secteur public existent pour fournir des services aux contribuables. Les risques surviennent quand la qualité des services rendus n'est pas celle promise, ou le niveau de service est insuffisant.
	Technologie de l'Information	Risques liés spécifiquement aux objectifs des TI, infrastructures etc. Par exemple: • Problèmes de sécurit • Disponibilité de la technologie (à jour) • Infrastructures des TI • Intégration/interface des systèmes • Efficacité des technologies, et • Obsolescence des technologies
	Niveau de service	Les organisations du secteur public existent pour fournir des services aux contribuables. Les risques surviennent quand la qualité des services rendus n'est pas celle promise, ou le niveau de service est insuffisant.
	Niveau de service	Les organisations du secteur public existent pour fournir des services aux contribuables. Les risques surviennent quand la qualité des services rendus n'est pas celle promise, ou le niveau de service est insuffisant.

Source du Risque	Catégories de Risque	Description
Interne (suite)	Technologie de l'Information	Risques liés spécifiquement aux objectifs des TI, infrastructures etc. Par exemple: • Problèmes de sécurité • Disponibilité de la technologie (à jour) • Infrastructures des TI • Intégration/interface des systèmes • Efficacité des technologies, et • Obsolescence des technologies
	Performance des Tiers, Sous-traitants	Risques liés à la dépendance vis-vis des tiers, sous-traitants. Par exemple: • Performance insuffisante • Services rendus en retard • Problèmes de qualité
	Santé et Sécurité	Risques liés à la santé et sécurité (ex. accident de travail, déclaration d'une maladie dans l'institution)
	Plan de remise en état en cas de Sinistre/ Continuité des affaires	Risques liés à la non préparation ou l'absence d'un plan de remise en état pouvant ainsi nuire au bon fonctionnement après un sinistre (ex. désastre naturel, actes de terroristes, etc.) Ceci amène une interruption dans le processus de production et pourrait possiblement interrompre les opérations jusqu'à la remise en fonction des installations. Les facteurs à inclurent: • Procédures en cas de sinistres, et • Plan de crise
	Conformité/ Législation	Risques liés aux exigences de conformité. Par exemple: • Mécanismes d'application et supervision • Conséquences de la non-conformité, et • Contraventions ou pénalités payées
	Fraude et Corruption	Risques liés aux actes illégaux ou irréguliers commis par des employés et résultant en une perte d'actifs ou de ressources
	Financier	Risques englobant l'étendue de la gestion financière en général (à l'exception de la qualité de l''information financière). Quelques exemples: • Cash-flow et sa gestion • Pertes financières • Dépenses injustifiées • Allocations budgétaires • Collecte des revenus • Augmentation des dépenses opérationnelles
	Culturel	Risque liés à la culture d'entreprise dans son ensemble et l'environnement de contrôle. Quelques exemples: • Canaux de communication et leur efficacité • Intégration culturelle • L'éthique et les valeurs • Style de gestion

Exemple générique d'une Classification des Risques (Taxonomie) dans le secteur public

Source du Risque	Catégories de Risque	Description
Externe	Environnement Économique	Risques liés à l'environnement économique. Quelques exemples: • Inflation • Fluctuation dans les taux de change, • Taux d'intérêts
	Environnement Politique	Risques émanant de facteurs politiques et décisions ayant un impact sur le mandat et les opérations de l'institution. Quelques exemples: • Troubles politiques • Élections nationales, provinciales, locales
	Environnement Social	Risques liés à l'environnement social de l'institution. Quelques exemples: • Le chômage, sous-emploi, • Situation émigration/immigration
	Environnement Naturel	Risques liés à l'environnement naturel et son impact sur les opérations. Quelques exemples: • Épuisement des ressources naturelles • Dégradation environnementale • Pollution
	Environnement Technologique	Risques émanant des effets des avancements et changements dans la technologie.
	Environnement Législatif	Risques relatifs à l'environnement législatif de l'institution. (ex. Changements dans la législation, réglementation, etc.)

Exemple - Les risques liés à la responsabilité sociale de l'entité

E.1. Les valeurs fondamentales adoptées par les nations unies dans la déclaration du millénaire

En 2000, l'Assemblée générale des Nations Unies a adopté la déclaration du Millénaire, dans laquelle les Etats membres ont exprimé leur attachement à certaines valeurs fondamentales qui doivent sous-tendre les relations internationales au XXIe siècle :

Objectif 1 : Réduire l'extrême pauvreté et la faim
Réduire de moitié, entre 1990 et 2015, la proportion de la population dont le revenu est inférieur à 1 dollar par jour,
Réduire de moitié, entre 1990 et 2015, la proportion de la population qui souffre de la faim.

Objectif 2: Assurer l'éducation primaire pour tous
Donner, d'ici à 2015, à tous les enfants, garçons et filles, les moyens d'achever un cycle complet d'études primaires.

Objectif 3: Promouvoir l'égalité des sexes et l'autonomisation des femmes
Éliminer les disparités entre les sexes dans l'enseignement primaire et secondaire, de préférence avant 2005, et à tous les niveaux de l'enseignement au plus tard en 2015.

Objectif 4 : Réduire la mortalité infantile
Réduire de deux tiers, entre 1990 et 2015, le taux de mortalité des enfants de moins de 5 ans.

Objectif 5 : Améliorer la santé maternelle
Réduire de trois quarts, entre 1990 et 2015, le taux de mortalité maternelle

Objectif 6: Combattre le VIH/Sida, le paludisme et d'autres maladies
Stopper la propagation du VIH/ sida d'ici à 2015 et commencer à inverser la tendance actuelle,
Stopper, d'ici 2015, l'incidence du paludisme et d'autres grandes maladies et commencer à inverser la tendance actuelle.
Objectif 7 : Assurer un environnement durable
Intégrer les principes du développement durable, dans des politiques nationales; inverser la tendance actuelle à la déperdition des ressources environnementales, Réduire de moitié d'ici à 2015 le pourcentage de la population qui n'a pas accès de façon durable à un approvisionnement en eau potable et en assainissement de base.

Objectif 8 : Mettre en place un partenariat mondial pour le développement
Poursuivre la mise en place d'un système commercial et financier multilatéral ouvert, fondé sur des règles, prévisible et non discriminatoire. Cela suppose un engagement en faveur d'une bonne gouvernance, du développement et de la lutte contre la pauvreté, au niveau tant national qu'international,
S'attaquer aux besoins particuliers des pays les moins avancés. La réalisation de cet objectif suppose l'admission en franchise et hors contingents de leurs exportations, l'application du programme renforcé d'allégement de la dette des pays pauvres très endettés (PPTE), l'annulation des dettes bilatérales entre les créanciers officiels et l'octroi d'une aide publique au développement plus généreux aux pays qui démontrent leur volonté de lutter contre la pauvreté,
Répondre aux besoins particuliers des États sans littoral et des petits États insulaires en développement,
Traiter globalement le problème de la dette des pays en développement par des mesures d'ordre national et international propres à rendre leur endettement viable à long terme,
En coopération avec les pays en développement, créer des emplois décents et productifs pour les jeunes,
En coopération avec l'industrie pharmaceutique, rendre les médicaments essentiels disponibles et abordables dans les pays en développement,
En coopération avec le secteur privé, mettre les avantages des nouvelles technologies, en particulier des technologies de l'information et de la communication, à la portée de tous.

E.2. Les objectifs de développement durable

«Nous n'héritons pas de la terre de nos ancêtres, nous l'empruntons à nos enfants***».***

Antoine de SAINT-EXUPERY

La définition classique du développement durable provient du Rapport BRUNDTLAND: « *Le développement durable est un développement qui répond aux besoins du présent sans compromettre la capacité des générations futures de répondre aux leurs. Deux concepts sont inhérents* à *cette notion: le concept de besoins, et plus particulièrement des besoins essentiels des plus démunis,* à *qui il convient d'accorder la plus grande· priorité, et l'idée des limitations que l'état de nos techniques et de notre organisation sociale impose sur la capacité de l'environnement* à *répondre aux besoins actuels et* à *venir».*

➡ **On peut considérer que les objectifs se partagent entre trois grandes catégories:**
- Ceux qui sont traités à l'échelle de la planète: rapports entre nations, individus, générations,
- Ceux qui relèvent des autorités publiques dans chaque grande zone économique (Union européenne, Amérique latine, Asie, Afrique...), à travers les réseaux territoriaux par exemple,
- Ceux qui relèvent de la responsabilité des entités.

E.3. LE PACTE MONDIAL ?

Le Pacte mondial est un pacte proposé par Kofi ANNAN, une initiative internationale où il est demandé aux grandes entreprises de se joindre à la société civile et aux organismes de l'ONU afin de supporter dix principes dans les domaines de l'environnement, des droits de l'homme et des droits du travail.

Le pacte est un code de conduite que les entités du secteur privé doivent s'engager à respecter et à mettre en pratique. Le Pacte mondial, connu en anglais sous le terme ***Global compact*** fut initié lors du Forum économique mondial en janvier 2000 et n'est pas juridiquement contraignant.

➥ **Les dix principes du Pacte sont inspirés :**

- de la ***Déclaration universelle des dro***its de l'homme,
- **de la *déclaration relative aux principes et droits fondamentaux au travail*** (Organisation internationale du travail),
- de la ***décla***ration de Rio sur l'environnement et le développement,
- et de la ***Convention des Nations Unies contre la corruption (***Le dixième principe concernant la corruption fut ajouté en 2004).

Les dix principes du Pacte mondial

Droits de l'homme

- ✓ **Principe 1** : Promotion et respect des droits de l'homme reconnus sur le plan international;
- ✓ **Principe 2** : Non-complicité de violations des droits fondamentaux.

Normes de travail

- ✓ **Principe 3** : Respect de l'exercice de la liberté d'association et reconnaissance du droit à la négociation collective;
- ✓ **Principe 4** : Élimination de toutes les formes de travail forcé et obligatoire;
- ✓ **Principe 5** : Abolition effective du travail des enfants;
- ✓ **Principe 6** : Élimination de la discrimination en matière d'emploi et d'exercice d'une profession.

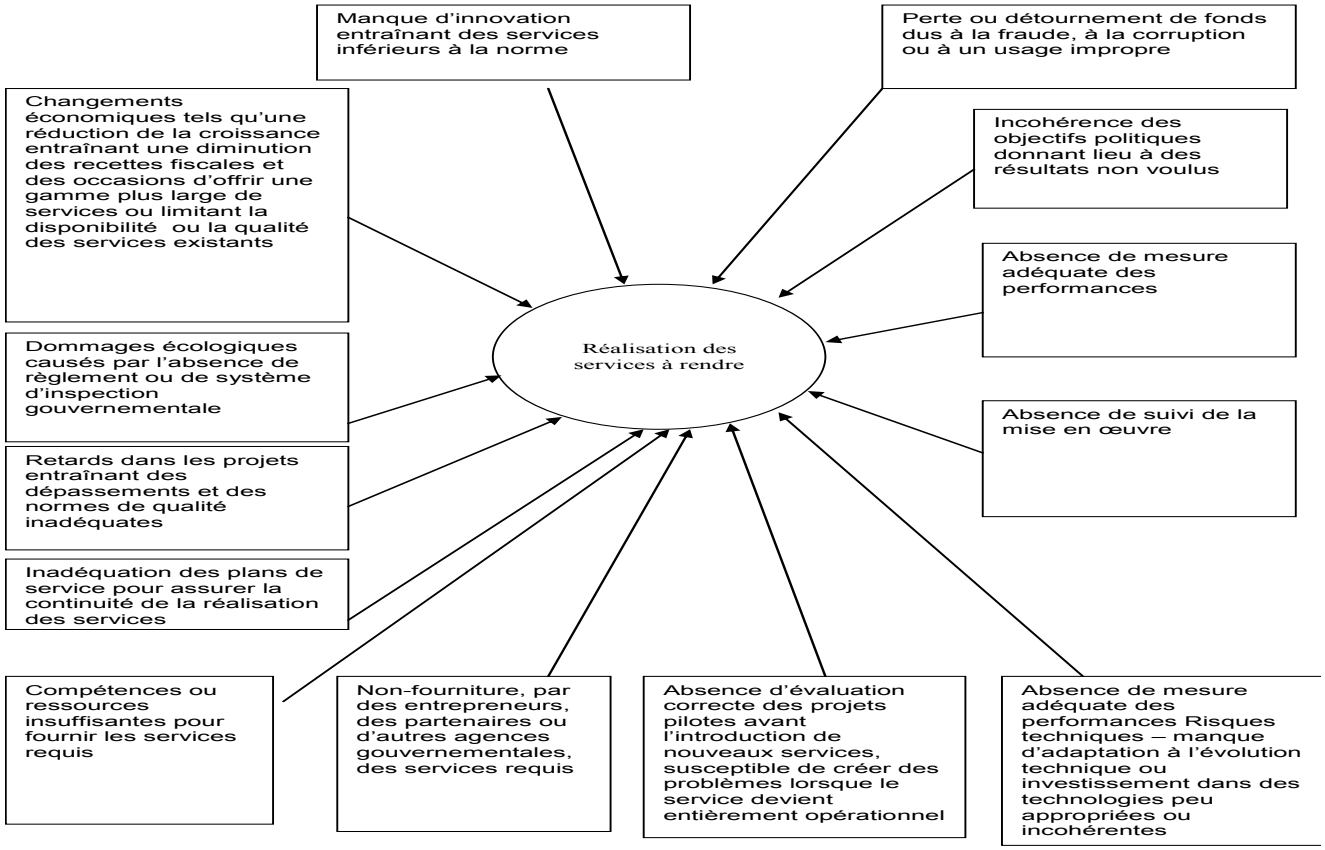
Environnement

- ✓ **Principe 7**: Promotion d'une approche prudente des grands problèmes touchant l'environnement;
- ✓ **Principe 8** : Prise d'initiatives en faveur de pratiques environnementales plus responsables;
- ✓ **Principe 9**: Encouragement à la mise au point et la diffusion de technologies respectueuses de l'environnement.

Lutte contre la corruption

- ✓ **Principe 10**: Action contre la corruption sous toutes ses formes, y compris l'extorsion de fonds et les pots-de-vin.

Risques caractéristiques auxquels les organisations publiques sont confrontées



Remarques : 15 Catégories de risques sont retenues dans le modèle proposé

1. Risque Economique
2. Risque Stratégique
3. Risque Financier
4. Risque Opérationnel
5. Risque Informatique
6. Risque Ressource Humaine
7. Risque de fraude, corruption, détournement
8. Risque qualité du service
9. Risque qualité de l'information
10. Risque Juridique
11. Risque d'Image /réputation
12. Risque d'intégrité
13. Risque de Défaillance
14. Risque d'approvisionnement
15. Risque Environnemental

Etape 2.2 Création d'une échelle de cotation des risques et mise en œuvre (quantification ou cotation)

La Quantification ou cotation des Risques : Mesure du risque: Quantifier la vulnérabilité du ministère ou de l'entité face au risque par l'évaluation de:

- l'impact possible du risque et
- sa probabilité de survenance ou occurrence.

⇨ La Quantification des Risques – Evaluation de l'Impact[15]

Score - Evaluation	5- Critique	4- Majeur	3- Modéré	2- Mineur	1 - Non significatif
Echelle d'impact sur l'objectif					
Description de l'impact sur l'objectif	Risque ayant une importance critique sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact relativement substantiel sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact relativement modéré sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact faible sur la capacité d'atteinte de l'objectif de gestion	Risque ayant un impact négligeable sur la capacité d'atteinte de l'objectif de gestion
Echelle d'impact sur l'image					
Durée de l'atteinte à l'image (vis-à-vis de l'opinion publique, d'organismes internationaux ou nationaux, des Partenaires Techniques et Financiers (PTF))	Crédibilité gravement affectée à long terme (>3 ans)	Crédibilité gravement affectée à moyen terme (>1 an)	Crédibilité affectée à court terme (> 3 mois)	Crédibilité affectée à court terme (> 1 semaine)	Crédibilité affectée pendant moins d'une semaine
Echelle d'impact financier					
Impact financier F CFA	**> 10 000 000 CFA**	**1 000 000 à 10 000 000 CFA**	**100 000 à 1 000 000 CFA**	**10 000 à 100 000 CFA**	**< 10 000 CFA**
Echelle d'impact Humain					
Impact humain (conditions sociales, de travail,…)	Impact ayant une importance critique sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact relativement substantiel sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact relativement modéré sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact faible sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).	Impact négligeable sur les agents de l'entité (surcharge de travail, stress, démotivation, accidents de travail, maladies...).

Echelle d'impact sur les clients/partenaires					
Impact sur les clients/ partenaires	impact très important sur les parties prenantes externes : clients/usagers/ bénéficiaires, fournisseurs, PTF, investisseurs, etc.	impact relativement significatif sur les parties prenantes externes : clients/usagers/bénéficiaires , fournisseurs, PTF, investisseurs, etc.	impact significatif sur les parties prenantes externes : clients/usagers/bénéficiaires , fournisseurs, PTF, investisseurs, etc.	impact faible sur les parties prenantes externes : clients/usagers/bénéficiaires , fournisseurs, PTF, investisseurs, etc.	impact négligeable sur les parties prenantes externes : clients/usagers/bénéficiaires , fournisseurs, PTF, investisseurs, etc.

[15] Considération faite des facteurs qualitatifs et/ou quantitatifs

⧫ L'impact peut donc concerner :

a) **l'Humain** : sur les travailleurs (surcharge de travail, stress, démotivation, accidents de travail, maladies...).
b) **le Financier** : pertes financières (ressources en moins)
c) **l'Image** : réputation.
d) **les relations avec les Clients/partenaires, usagers** : impact sur les parties prenantes externes : clients/usagers/bénéficiaires, fournisseurs, Etat, régulateurs, investisseurs, revendicateurs, etc.
e) **la technique** : dysfonctionnements, impact sur la continuité du processus, sur les activités, sur les produits/services, sur la qualité et les délais.

⧫Quelques facteurs permettant de mesurer l'impact :

- Matérialité
- Conséquences financières
- Conséquences humaines
- Visibilité et degré d'implication des instances dirigeantes

⇨ **La Quantification des Risques – Probabilité de Survenance ou occurrence (critères qualitatif/ quantitatif)**

Echelle de probabilité des risques					
Niveau de probabilité	**Très probable 5**	**Probable 4**	**Modérément probable 3**	**Peu probable 2**	**Rare 1**
Description	Le risque s'est manifesté fréquemment et se manifestera très probablement plus d'une fois dans les 12 prochains mois	Le risque est courant. Il a une chance importante de se manifester au moins une fois dans les 12 prochains mois	Le risque a une chance au-dessus de la moyenne de se manifester au moins une fois dans les 3 prochaines années	Le risque est très peu fréquent, et peu probable de survenir dans les 3 prochaines années	Le risque est concevable mais il n'est susceptible de se manifester que dans circonstances extrêmes
Critères qualitatifs (orientés fraudes, malveillances,…)					
Motivation	Enrichissement personnel ou motifs idéologiques	Nuire à l'institution	Nuire à la bonne marche d'un service ou d'un processus	Nuire à la hiérarchie ou à ses collègues	Attirer l'attention (satisfaire son égo)
Critères qualitatifs (orientés erreurs, incidents opérationnels,…)					
Sensibilisation et compétence des personnels	Aucune culture du risque et du contrôle interne. Personnels de différents profils avec des compétences et une expérience faibles. Absence de formation	Faible culture du risque et du contrôle interne. Personnels différents profils avec des compétences et ne expérience de base. Formation de base	Culture limité du risque et du contrôle interne. Personnels de différents profils avec des compétences et une expérience standard. Formation standard	Forte culture du risque et du contrôle interne. Personnels de différents profils avec des compétences et une expérience avancées. Formation spécialisée	Très forte culture du risque et contrôle interne. Personnels expérimentés avec une réelle expertise. Formation continue de haut niveau

⧫ Quelques facteurs influençant la probabilité ou l'occurrence de survenance :

- Complexité des opérations
- Antécédents et réputation
- Compétence
- Stabilité et réforme
- Liquidités des actifs

Etape 2.3 La Quantification ou cotation des Risques Inhérents – (Impact x Probabilité) pour chaque ensemble homogène et formalisation des résultats dans une matrice des risques bruts ou inhérents (Etape 2.4)

Risque brut ou inhérent: L'exposition au risque en terme absolu avant prise en considération des mesures de contrôle interne

Score Combiné (IxP)	Ampleur du Risque Inhérent	Réponse et Traitement du Risque
15 - 25 **(rouge)**	**ELEVE**	**Niveau de risque inacceptable– nécessité de maintenir un haut niveau de contrôle pour réduire le risque résiduel à un niveau acceptable**
8 - 14 **(jaune)**	**MOYEN**	**Niveau de risque inacceptable, excepté sous certaines conditions – un niveau modéré de contrôle est nécessaire pour réduire le risque résiduel à un niveau acceptable**
1 - 7 **(vert)**	**FAIBLE**	**Généralement acceptable – un niveau faible de contrôle voire une absence de contrôle peut être autorisé**

Etape 2.5 La définition de l'ensemble des Bonnes pratiques de Contrôle interne communément admises de maîtrise des risques qui devront exister.

⇨ **Matrice des Risques Inhérents (ou registre) – Cartographie du Risque inhérents**

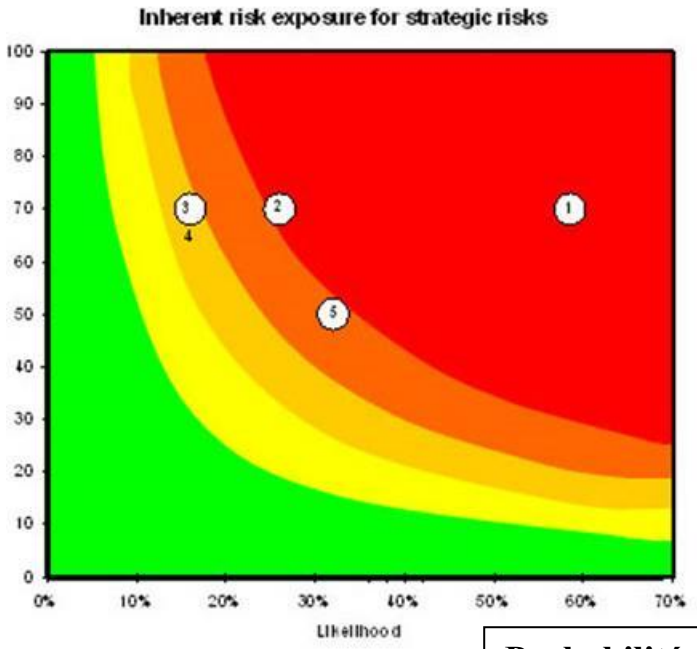
Département :
Objectif(s) Départementaux
1. Xx
2. Xx

Réf	Réf. domaines, Missions, activités, tâches	Risques potentiel (par rapport objectifs gestion et du CI)	Catégorie de risque (15 catégories)	Analyse Causale (par rapport composants du CI)	Responsables	Risque Inhérent			Bonnes pratiques de CI de maîtrise des risques
						Prob	I	Score / CR ou poids	
	Environnement de contrôle et pilotage (processus de pilotage stratégique et opérationnel)								
	Processus Métier								
	Processus d'appui								

⇨ **Représentation Graphique du Risque Inhérent – Cartographie du Risque**

La cartographie (ou Heat Map) permet de :
- Visualiser les risques acceptables et non acceptables
  - individuellement
  - en relations l'un par rapport à l'autre
  - en groupes ou sous-groupes

Impact



Probabilité

Les différentes méthodes de traitement des Risques

Traitement – mise en place de contrôles efficaces

Tolérance – Pas d'action supplémentaires, le risque se trouve dans les limites convenues, la probabilité est extrêmement basse ou le coût du traitement dépasse le bénéfice attendu

Transfert -Passer le risque à d'autres institutions, par exemple, une assurance contre le risque, un partenariat, une sous-traitance ou contractualisation du risque

Terminer : Suppression – Abandon de l'activité risquée

FICHE N°9 Identification et évaluation du contrôle interne

1. Rappel de la définition du contrôle interne

C'est « le processus mis en œuvre par la direction générale, la hiérarchie, le personnel d'une entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- La réalisation et l'optimisation des opérations,
- La fiabilité des informations,
- Respect des réglementations en vigueur
- La protection des ressources

2. La démarche et les outils d'évaluation du contrôle interne

Etape 3 : Identification et évaluation de la maturité du contrôle interne

1. Pour chaque ensemble homogène, et au regard de chaque risque, identifier les dispositifs de contrôle interne clefs en place (Matrice d'évaluation de la qualité du contrôle interne, **Réf. 11 Kit, ou Matrice des risques et contrôle, Réf. 13 Kit). (Tâche 1).**

2. De procéder à la cotation de la qualité du contrôle interne par rapport à sa capacité de prévenir à protéger donc à maîtriser les risques identifiés : adéquation de la conception et efficacité des contrôle (Matrice d'évaluation de la qualité du contrôle interne, **Réf. 11 Kit, ou Matrice des risques et contrôle, Réf. 13 Kit**). **(Tâche 2).**

Par exemple une échelle de 4 en fonction des critères suivants :
* 0 à 3 pour la prévention : Qualité du dispositif de prévention des risques (formation, sensibilisation, contrôles, etc.)
* 0 à 3 pour la Qualité du dispositif de protection contre les impacts des risques : pilotage institutionnel performant, formalisation des procédures et diffusion, procédures appliquées et mises à jour, compétence suffisante, diffusées (détection, correction)

3. Procéder à une cotation des dispositifs de CI existants **(Tâche 3) : capacité à réduire la probabilité des risques (prévention) et / ou à réduire l'impact (protection) : appréciation globale du CI sur une grille de 1 à 5**

Une note de (voir grille d'évaluation de la maturité du ci- après):

- 1 est attribuée pour un CI non ou peu fiable
- 2 est attribuée pour un CI informel
- 3 est attribuée pour un CI standardisé
- 4 est attribuée pour un CI maîtrisé ou surveillé
- 5 est attribuée pour un CI optimisé

4. Cette étape **aboutit à la formalisation des résultats dans une maitrise d'évaluation du CI** (Rapport type élaboration cartographie et plan **d'ABR Réf. 16 Kit**). **(tâches 4)**

⇨ **Livrables Etape 3 (tâches 4) :** **Matrice d'évaluation du CI**

<u>Cotation du niveau de maturité du CI, échelle de 1 à 5</u> : qui définit la qualité, l'efficacité, la pertinence, la fiabilité, et l'efficience du dispositif de contrôle interne mise place et selon un code couleur lié à sa gravité

Niveau	Qualité	Commentaire sur la maturité du CI (Qualité du dispositif du contrôle interne)
5 (Vert)	**Optimisé**	Les activités de contrôle sont coordonnées et la gestion des risques est conduite dans un système intégré
4 (Jaune)	**Maîtrisé ou surveillé**	Les activités de contrôle sont décrites en détail et les contrôles sont effectifs. Il y a un responsable du CI et des vérifications sont faites régulièrement
3 (Jaune)	**Standardisé**	Des lignes directrices ont été mises en place, les processus sont documentés et les contrôles sont adaptés
2 (Rouge)	**Informel**	Les activités de contrôle interne sont mises en place mais sans standardisation. Ils dépendent des individus
1 (Rouge)	**Non ou peu fiable**	Peu ou pas d'activités de contrôle interne sont mises en place. L'organisation est à risque

<u>Grille d'évaluation de la prévention</u>

Niveau	Qualité de la prévention	Commentaire sur le CI
0	Aucune mesure de prévention n'existe (Prévention inexistante), ou il manque une mesure importante, ou les mesures sont inadaptées ou non mises en œuvre (Prévention inadaptée et ou Inefficace)	Qualité du Contrôle interne clef très faible, induisant une probabilité du risque très élevée (risque certaine) d'occurrence
1	Il existe des mesures de prévention peu ou moyennement adaptées et/ ou moyennement ou peu efficaces (Prévention peu ou moyennement adaptée et ou efficace)	Qualité du Contrôle interne clef moyenne induisant une probabilité du risque modérée (quasi certaine ou probable) d'occurrence
2	Il existe des mesures de prévention adaptées qui sont mises en œuvre (Prévention adaptée et efficace)	Qualité du Contrôle interne clef élevé induisant une probabilité du risque faible (ou peu probable) d'occurrence
3	Il existe des mesures de prévention très adaptées qui sont efficacement mises en œuvre et pour lesquelles on assure une traçabilité, un suivi et un contrôle (Prévision très adaptée et efficace)	Qualité du Contrôle interne clef très élevé induisant une probabilité du risque très faible (ou quasi impossible) d'occurrence

Grille d'évaluation de la protection:

Niveau	Qualité de la protection	Commentaire sur le CI
0	Aucune mesure de protection n'existe, ou il manque une mesure importante, ou les mesures sont inadaptées ou non mises en œuvre (Protection inexistante, inadaptée et ou Inefficace)	Contrôle interne clef n'offrant aucun effet protecteur (réducteur) sur l'impact du risque sur les objectifs
1	Il existe des mesures de Protection moyennement ou peu adaptées et ou efficaces (Protection moyennement ou peu adaptée et ou efficace)	Contrôle interne clef ayant un effet protecteur (réducteur) modéré ou moyen sur l'impact du risque
2	Il existe des mesures de Protection adaptées qui sont mises en œuvre (Protection adaptée et efficace)	Contrôle interne clef ayant un effet protecteur (réducteur) sur l'impact du risque
3	Il existe des mesures de Protection très adaptées qui sont efficacement mises en œuvre et pour lesquelles on assure une traçabilité, un suivi et un contrôle (Protection très adaptée et efficace)	Contrôle interne clef ayant un effet protecteur (réducteur) maximum sur l'impact du risque

3. Matrice d'évaluation du Contrôle Interne (voir page suivante)

⇨Les contrôles internes mis en place pour maîtriser les risques peuvent être :

- Préventifs, détectifs ou de correctifs (ou a posteriori) et directif
- manuelles ou automatiques,
- Contrôle essentiel (contrôle clés et secondaire)
- Contrôle complémentaire ou contrôle de compensation
- s'effectuent au niveau de l'entité, du processus, ou au niveau des opérations (transactions)

⇨ ***Rappel :*** **Quelques exemples des activités de contrôle les plus courantes décrites par le COSO :**

- **Revues du management**, tels les examens du respect du budget, l'actualisation des prévisions, la surveillance des actions ou des initiatives de maîtrise des coûts.
- **Supervision directe d'une activité ou d'une fonction** par les responsables de fonctions ou d'activités spécifiques, par exemple vérification des rapports analytiques de gestion, rapprochements.
- **Traitement de l'information.** Contrôles conçus pour vérifier l'exactitude, l'exhaustivité et la validation des transactions, tels que :
  - les contrôles généraux de l'infrastructure,
  - la sécurité physique et logique,
  - les contrôles sur la mise en œuvre des systèmes,
  - les évolutions de versions ou les modifications,
  - la reprise après sinistre et les contrôles des opérations issues des systèmes.
- **Contrôles physiques :**
  - (1) l'inventaire physique des espèces, des titres, des stocks, du matériel et des autres immobilisations, et la comparaison du résultat de cet inventaire avec les chiffres enregistrés dans les comptes et les dossiers
  - et (2) les obstacles ou restrictions physiques, tels que les barrières et les verrous.
- **Indicateurs de** performances : analyse des écarts entre prévisions et réalisations.
- **Séparation des** tâches incompatibles afin de limiter le risque d'erreur ou de fraude.

⇨Le chiffrage de la qualité ou maturité du contrôle interne (dispositifs de prévention, de protection, de détection et de correction afin de faire face aux risques identifiés) repose sur les critères ci-après :

- **Efficacité**: capacité du contrôle clés à jouer pleinement son rôle et à atteindre les résultats pour lesquels il est mis en œuvre
- **Pertinence (adéquation)**: utilité du contrôle clés, adapté au risque à maîtriser.
- **Fiabilité**: capacité du contrôle clés à fonctionner correctement de façon permanente.
- **Qualité** de la conception et de la mise en œuvre du contrôle clés
- **Efficience**: coût/résultats/délais d'obtention des résultats.

⇨ La réalisation des tests suivants permet de s'assurer de l'adéquation de la conception et de l'efficacité des contrôles clés :

1. existence des bonnes pratiques (des contrôle internes clés conformes aux bonnes pratiques)
2. pertinence (adéquation), de la qualité de la conception, de la qualité de l'application et de l'efficacité de la mise en œuvre des bonnes pratiques (prise en compte des incidents : historique)
3. existence de dispositifs alternatifs (dispositifs mis en place en l'absence des bonnes pratiques).
4. pertinence (adéquation), de la qualité de la conception, de la qualité de l'application et de l'efficacité de la mise en œuvre de ces dispositifs alternatifs.

L'évaluation globale et la cotation du dispositif de maîtrise des risques intervien à la fin des tests ci- dessus. Une validation avec les opérationnels permet de conclure sur la qualité réelle du Contrôle interne.

MATRICE D'EVALUATION DU CONTROLE INTERNE (évaluation des contrôles internes clés existants : Tableau des forces et des faiblesses apparentes)				
ELEMENTS (OU COMPOSANTS) DE CONTROLE INTERNE	**DOCUMENTATION PERTINENTE UTILES OU CONTROLES INTERNES CLES EXISTANTS (Bonnes pratiques)** **Nota : Les contrôles internes clés garantissent l'atteinte des objectifs de gestion de l'entité à travers les 4 sous objectifs suivants : Sécurité des ressources, respect des lois et des règlements, fiabilité de l'information, optimisation des performances (5 E)**	**Existence**		**Cotation du niveau de maturité du contrôle Interne : Prévention (3) et Protection (3) = Niveau de maturité CI 1 à 5**
		Oui	**Non ou N/A**	
1. OBJECTIFS CLAIREMENT DEFINI ET DECLINES DE HAUT EN BAS	• Textes Fondateurs • Document de politique générale • Plan stratégique • Programme d'activités • CDMT global ou sectoriel • Dispositions législatives • Lettre de mission • Contrats d'objectifs • Indicateurs correspondant aux objectifs • tableaux de bord • Code d'éthique • PV conseil de discipline • Plan d'action • Autres à préciser			
2. ORGANISATION ADAPTEE	• Organigramme général • Organigramme détaillé • Fiche de description des postes • Compte rendu des réunions des organes de gouvernance (PV). • Délégation des pouvoirs			
3. MOYENS EN ADEQUATION AVEC LES OBJECTIFS	• Moyens humains : o qualité o quantité • Plan de formation • Motivation • Système d'évaluation individuel annuel • Moyens matériels (bureautique) o qualité o quantité • Moyens matériels (autres, à préciser) • Moyens financiers			
4. PROCEDURES FORMALISEES COUVRANT TOUTES LES FONCTIONS ET APPLIQUEES	• Manuel de procédure • Notes de procédures ou guide des tâches • Manuel d'exécution • Cartographie des processus • Fréquence des mises à jour.			
5. SYSTEME D'INFORMATION PERTINENT COUVRANT TOUTES LES FONCTIONS ET PRODUISANT DES INFORMATIONS FIABLES, PERTINENTES, EXHAUSTIVES, DISPONIBLES A TEMPS	• Comptabilité générale • Comptabilité budgétaire • Comptabilité analytique • Comptabilité matières • Indicateurs clés par direction et par processus et tableaux de bord • planning des reporting • Rapport d'activité • Schéma directeur informatique • Plan d'entretien • Gestion des habilitations. • Plan de secours, de continuité de l'exploitation, de sécurité. • Programme de formation des utilisateurs. • Etudes préalables. • Guides d'utilisateur.			

6. SUPERVISION PERTINENTE ET UNIVERSELLE (tout est supervisé et tout le monde est supervisé)	• Contrôle hiérarchique (autorisation, Réunion, sanctions) • Contrôle sur les processus par la hiérarchie (séparation des tâches et des fonctions, procédure de prévention et de détection, procédures de traitement des incidents) • Contrôle indépendant (y compris l'audit et l'inspection) • contrôle sur les transactions (recoupements, rapprochements, inventaires physiques, etc.)			

Nota : Ces éléments classiques peuvent être repositionnés dans le COSO 1 révisé en 2013 (Fêtes l'exercice)

Composantes	Principes	
Environnement de contrôle	**1**	L'organisation démontre son engagement en faveur de l'intégrité et de valeurs éthiques.
	2	Le conseil d'administration fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne.
	3	La direction, agissant sous la surveillance du conseil d'administration, définit les structures, les rattachements, de contrôle ainsi que les pouvoirs et les responsabilités appropries pour atteindre les objectifs.
	4	L'organisation démontre son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs.
	5	L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne.
Evaluation des risques	**6**	L'organisation spécifie les objectifs de façon suffisamment claire pour permettre l'identification et l'évaluation des risques associés aux objectifs.
	7	L'organisation identifie les risques associés à la réalisation de ses objectifs dans l'ensemble de son périmètre de responsabilité et elle procède à leur analyse de façon à déterminer les modalités de gestion des risques appropriées.
	8	L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles de compromettre la réalisation des objectifs.
	9	L'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle interne.
Activités de contrôle	**10**	L'organisation sélectionne et développe les activités de contrôle qui contribuent à ramener à des niveaux acceptables les risques associés à la réalisation des objectifs.
	11	L'organisation sélectionne et développe des activités de contrôle général en matière de système d'information pour faciliter la réalisation des objectifs.
	12	L'organisation met en place les activités de contrôle par le biais de directives qui précisent les objectifs poursuivis et de procédures qui mettent en œuvre ces directives.
Information et communication	**13**	L'organisation obtient ou génère puis utilise des informations pertinentes et de qualité pour faciliter le fonctionnement des autres composantes du contrôle.
	14	L'organisation communique en interne les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne, notamment en ce qui concerne les objectifs et les responsabilités associés au contrôle interne.
	15	L'organisation communique avec les tiers au sujet des facteurs qui affectent le bon fonctionnement des autres composantes du contrôle interne.
Pilotage	**16**	L'organisation sélectionne, met au point et réalise des évaluations continues et/ou ponctuelles afin de vérifier si les composantes du contrôle interne sont bien mises en place et fonctionnent.
	17	L'organisation évalue et communique les faiblesses de contrôle interne en temps voulu aux responsables des mesures correctrices, notamment à la direction générale et au conseil d'administration.

Cartographie des risques (Forces et faiblesses apparentes du CI par rapport aux risques inhérents)

Réf.	Réf. et domaines auditables (les missions) : Processus, sous processus, missions, activités, tâches	Identification des Risques potentiels (par rapport objectifs du CI)	Catégorie de risque (15 catégories)	Analyse Causale (par rapport composants du CI)	Responsables (propriétaires des risques et client, fournisseur, appui)	Risque Inhérent			Bonnes pratiques de CI de maîtrise des risques	Identification des Contrôles Internes Clefs pour mitiger le risque		Evaluation des Contrôles Internes Clefs existants (Pro et Pré) = Maturité du CI		
						Prob	I	Score P*I		Existants (forces apparentes)	Inexistants (faiblesses apparentes)	Pré	Pro	Niveau de maturité CI 1 à 5
	Environnement de contrôle et gouvernance													
	Processus Métiers													
	Processus d'appui													

4. Traitement des Risques par les Activités de Contrôle Interne

Le contrôle interne est le principal mécanisme de traitement des risques.

Contrôles internes: Procédés destinés à aider le ministère à accomplir ses objectifs de gestion par le biais de :

- Structure organisationnelle
- Répartition des tâches
- Délégations de pouvoir
- Qualité du personnel
- Systèmes de gestion de l'information

Les 2 catégories de systèmes de la nouvelle gestion publique :

Contrôle interne
=
Contrôle interne financier (budgétaire et comptable)
+
Contrôle interne de gestion

FICHE N°10 — Evaluation des risques résiduels

1. La démarche

Etape 4 : Evaluation des risques résiduels

La dernière étape est d'évaluer avec les propriétaires des risques dans quelle mesure **le système de contrôle interne en place réduit le niveau du risque inhérent (probabilité/prévision ou impact/protection)**.

1. En rapprochant, pour chaque « ensemble homogène », la matrice des risques bruts de celle concernant l'évaluation du contrôle interne, l'auditeur détermine **les risques résiduels (filtrés par le CI)**, il peut être déduit **une cartographie des risques résiduels** (non couvert ou mal couvert par un dispositif de CI absent ou défaillant) **: (Tâche 1).**

2. On obtient en final une cartographie des risques pour toute l'organisation découpée en métier, entité et processus **(Tâche 2).**

- **Nota : L'évaluation du risque résiduel est effectuée comme suit : score Risque résiduel égal :**

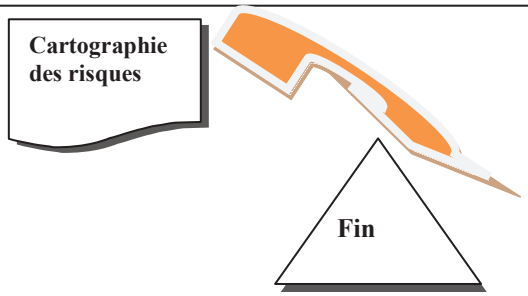
1. **L'Impact résiduel (= Impact risque inhérent – Niveau de Protection CI) :** c'est la différence entre la cotation de l'impact (I) du risque inhérent et la cotation du niveau de protection du CI (Pro).

Conditionnalité de la cotation de la protection : le niveau de la protection (dispositif de contrôle interne mis en place qui devrait agir sur l'impact ou la gravité d'un risque) **ne peut être supérieure ou égal (>=) à celui de l'impact du risque inhérent**, car elle ne permettra pas une couverture totale de la gravité du risque. Par conséquent, la cotation de la protection sera toujours inférieure (<) d'au moins **1 point** de celle de l'impact.

2. **la Probabilité résiduelle = Probabilité risque inhérent –niveau de la capacité du CI à Prévenir le risque :** c'est la différence entre la cotation de la probabilité du risque (risque inhérent) et la Cotation de la prévention (Pré).

Conditionnalité de la cotation de la prévention : le niveau de la prévention (dispositif de contrôle interne qui agit sur la probabilité ou l'occurrence d'un risque) **ne peut être supérieure ou égal (>=) à celui de la probabilité du risque inhérent,** car si le risque est survenu, c'est parce que le dispositif de contrôle est inefficace et/ou inadéquat. Par conséquent, la cotation de la **prévention sera toujours inférieure** (<) d'au moins **1 point** de celle de la probabilité.

Livrables Etape 4 : ⇨



⇨ REMARQUE

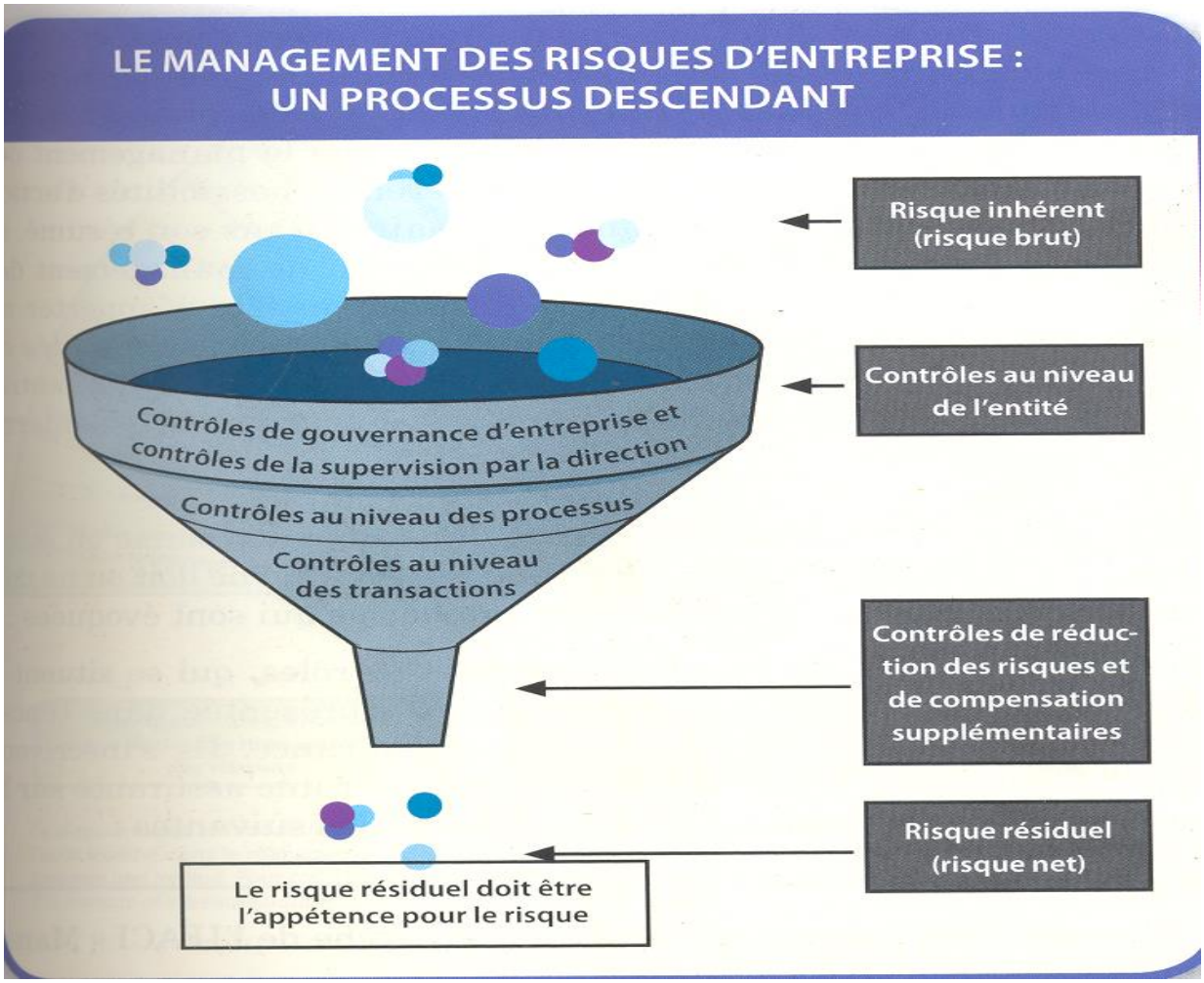
Le risque résiduel correspond au risque brut non couvert (ou mal) par un dispositif de contrôle interne absent (ou défaillant). Il est déduit sur la base de l'appréciation **des forces et faiblesses du dispositif de contrôle interne de l'entité (la qualité du CI amplifie ou atténue la probabilité et l'impact du risque brut)**.

En effet l'évaluation qualitative de la probabilité et de l'impact d'un risque est inversement proportionnelle ***à la qualité du contrôle interne.***

Niveau du contrôle interne	***Probabilité et impact du risque***
Elevé	*Faible*
Moyen	*Moyenne*
Faible	*Elevée*

La prévention a pour objectif de diminuer la probabilité ou la fréquence de survenance d'un sinistre. En revanche, elle peut être sans effet sur la gravité des sinistres potentiels.

Rappelons la différence fondamentale avec **la protection**. Celle-ci s'adresse, avant tout, à la gravité en cherchant à la contenir, sans préoccupation quant à la fréquence. En analyse systémique, on peut également dire que la ***prévention est l'action sur les causes***, et la ***protection est l'action sur les conséquences.***



2. Outils de cotation du risque résiduel

Risque résiduel : L'exposition au risque qui existe après considération des contrôles internes mis en place pour détecter ou prévenir ces risques

Score Combiné (IxP)	Ampleur du Risque Résiduel	Réponse et Traitement du Risque
15 - 25 (rouge)	**ELEVE**	**Niveau de risque résiduel inacceptable- les contrôles sont inadéquats (mauvais design) or inefficaces (mauvaise application). Contrôles nécessitent refonte complète ou efforts significatifs dans leur application. Le risque est soit Traité, Transféré ou terminé.**
8 - 14 (jaune)	**MOYEN**	**Niveau de risque résiduel inacceptable- les contrôles sont inadéquats (mauvais design) or inefficaces (mauvaise application). Contrôles nécessitent refonte ou plus d'efforts dans leur application. Le risque est soit Traité, Transféré ou terminé.**
1 - 7 (vert)	**FAIBLE**	**Risque résiduel généralement acceptable – requiert une amélioration minimale des contrôles, ou maintien en l'état. Le risque peut être toléré.**

3 L'appétence au risque du management

Il s'agit de déterminer au près du Management, le niveau d''appétence au risque (ou le niveau de risque accepté) qui représente le niveau de risque acceptable retenu par la hiérarchie dans l'attente des objectifs.

Il est établi sous forme de menu déroulant à quatre (04) Niveaux :

- Traiter
- Tolérer
- Transférer
- Terminer

4 Rang de priorité

Il s'agit d'apprécier le niveau de gravité du risque et donc son rang de priorité (résolution des problèmes), en deux temps :

1. Niveau de survenance ou de récurrence (expérience historique : survenu ou pas)
2. Niveau de gravité suivant une grille de 1 à 3

Rang de priorité	Niveau de Priorité	Explication de la vulnérabilité (commentaire)
1	Zone d'audit et de traitement des risques prioritaires (Action immédiate)	Risque inacceptable devant être mis immédiatement sous contrôle (plan d'audit/ plan d'action)
2	Zone d'amélioration (Attention immédiate)	Risque inacceptable, protection insuffisante appelant des actions de remédiation en moyen terme (plan d'action)
3	Zone d'observation (Réévaluation périodique)	Les actions déjà existantes permettent de maîtriser les risques identifiés. Les dispositifs en place doivent être suivis et entretenus

5. Modalités de traitement du risque résiduel (commentaires)

⇨ Pour les risques élevés, l'auditeur élabore une Feuille d'Analyse des risque (FAR, Réf. 15 Kit) précisant :

- Le problème
- La cotation du risque inhérent
- Le risque résiduel et sa cotation
- Les dysfonctionnements à l'origine du risque résiduel
- Les conséquences sur les objectifs de gestion de l'entité
- Les éléments de contrôle interne à mettre en place (plan de mitigation)
- Les missions proposée par l'audit (type –assurance ou conseil -, objet, durée).

La FAR est datée, signée par l'auditeur, l'audité et le superviseur (le cas échéant), lors de la séance de restitution sur site. Un Procès-verbal est dressé par l'auditeur qui constate les points d'accords sur les risques et les méthodes de mitigation retenues (**PV compte rendu réunion sur site, Réf. 8.2).**

En final, on obtient une cartographie des risques pour la globalité de l'organisation découpée en « ensembles homogènes » (« métiers », « entités », « processus »).

Des modalités de mitigation sont décidées par la Direction (décision quant à l'acceptation du risque résiduel ou la définition et la mise en œuvre de nouveaux dispositifs de prévention, de réduction ou de protection pour en assurer la maîtrise : assurance, dispositifs de contrôle interne...), (Rapport type élaboration cartographie et plan **d'ABR, Réf. 16 Kit).**

⇨ Un plan de management des risques (ou de mitigation) est élaboré et validé par la hiérarchie. Le plan de mitigation précise :

- Risques
- Cotation (et rang de priorité)
- Objectif (Activité/tâche)
- Action de remédiation (recommandation)
- Période retenue pour la mise en œuvre
- Responsable de l'action
- Coût estimatif

⇨ La cartographie aide à définir la valeur des mesures de contrôle:

- Là où aucun contrôle n'existe, mais devrait l'être (Vulnérabilité)
- Là où les contrôles réduisent la probabilité de survenance des risques
- Là où les contrôles évitent ou limitent les conséquences du risque(Impact)
- Aide à orienter le travail des auditeurs et inspecteurs internes dans le cadre d'une approche d'audit basée sur les risques.

Cartographie ou registre des risques (voir page suivante)

Cartographie ou registre des risques

Référentiel à utiliser pour évaluer le risque inhérent, le niveau de contrôle interne, le risque résiduel et les mesures de traitement du risque résiduel

Réf.	Mission/Objectifs/ Activités	Risque identifié	Type de risque	Causes	Conséquences probables	Entités impliquées (Propriétaire, Fournisseur, Client, Appui)	Risque Inhérent			Bonnes pratiques de CI de maîtrise des risques	Éléments clés du Contrôle interne existants ou inexistants	Évaluation du contrôle interne			Risque résiduel Nota : Tout score élevé fait l'objet de FRAP (Voir QCI)			Appétence pour le risque : - Traiter - Tolérer -Transférer - Terminer	Classement		Plan de management des risques		Plan d'audit			
							Impact(I) 1 à 5	Probabilité (P) 1 à 5	Score= PxI			Protection (Pro) 0 à 3	Prévention (Pré) 0 à 3	Niveau de maturité CI 1 à 5	Impact = I - Pro	Probabilité = P - Pré	Score		Déjà Survenu Oui/Non	Rang de priorité Échelle 1 à 3	Actions (Recommandations)	Période retenue pour mise en œuvre	Audit Proposé	Type de revue	Objectifs et Périmètre d'Audit	Effort d'Audit Indicatif (Jours/ hommes)
PROCESSUS DE PILOTAGE																										
ENVIRONEMENT DE CONTROLE																										
A- Les préalables au contrôle interne																										
Objectifs Généraux																										
A1																										
B- REGLES D'EXEMPLARITE ET D'INTEGRITE*: E& I*																										
B1																										
J GOUVERNANCE																										
J1																										
PROCESSUS METIERS																										
PM 1																										
PROCESSUS SUPPORTS OU DE SOUTIENS																										
PS 1																										

Remarques : <u>La Considération de la Qualité des Contrôles –le Risques Résiduels</u>

Risque résiduel: L'exposition au risque qui existe après considération des contrôles internes mis en place pour détecter ou prévenir ce risque.

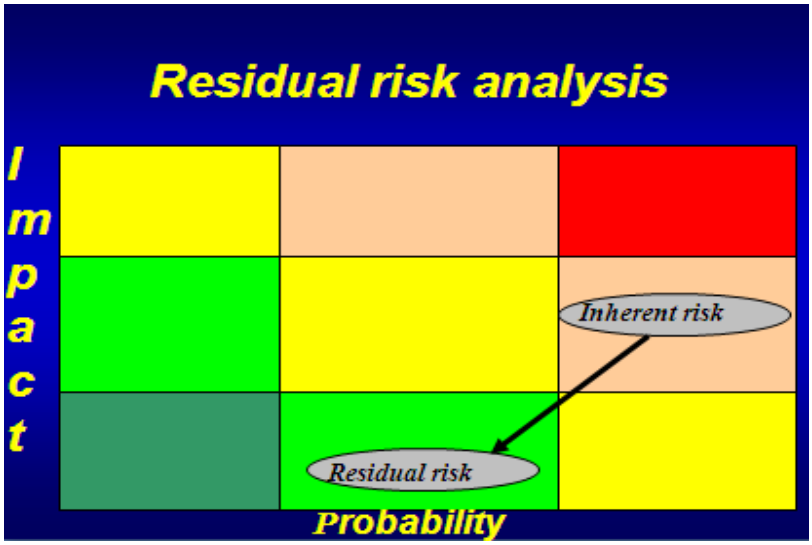
Pourquoi considérer le risque de cette manière ?

Aide à définir la valeur des mesures de contrôle :

- Là où aucun contrôle n'existe, mais devrait l'être (Vulnérabilité)
- Là où les contrôles réduisent la probabilité de survenance des risques
- Là où les contrôles évitent ou limitent les conséquences du risque(Impact)
- Aide à orienter le travail des auditeurs et inspecteurs internes dans le cadre d'une approche d'audit basée sur les risques.

⇨ **Représentation Graphique du Risque Résiduel – Cartographie du Risque**

La dernière étape est d'évaluer dans quelle mesure le système de contrôle interne en place réduit le niveau du risque inhérent. Ce graphique indique l'évolution du risque lorsque le contrôle interne est pris en compte.



Test de connaissances	QCM synthèse risques	Travaux de groupe

QCM de synthèse : Management et audit basés sur les risques

Test de Connaissances – Q1

1. Le but d'un référentiel de contrôle est:
    a. D'instaurer la discipline du contrôle interne à travers une organisation
    b. D'introduire une cohérence entre le risque et les concepts de contrôle à travers une organisation.
    c. De démontrer la relation entre le risque et le contrôle
    d. a, b, et c

Test de Connaissances – Q2

2. Le référentiel de contrôle du COSO :
    a. Est fondé sur un environnement de contrôle et une bonne gestion des risques
    b. Peut être appliqué dans toutes/tous les opérations/services du secteur public
    c. Est le modèle préféré pour le secteur public
    d. a, b, et c

Test de Connaissances – Q3

3. Une considération clef pour comprendre le risque est que:
    a. Le risque est de nature incertaine
    b. Le risque ne peut pas être géré
    c. Le risque est la responsabilité principale des auditeurs internes
    d. Aucune de ces réponses

Test de Connaissances – Q4

4. Une exposition aux risques avant d'envisager toute mesure de contrôle interne en place est considérée comme:
    a. Un risque stratégique
    b. Un risque résiduel
    c. Un risque inhérent
    d. Aucune de ces réponses

Test de Connaissances – Q5

5. Les contrôles internes sont essentiellement mis en place pour:
    a. Supprimer les risques
    b. Accepter les risques
    c. Réduire les risques
    d. Transférer les risques

Test de Connaissances – Q6

6. Lequel de ces risques n'est pas un risque du secteur public?
    a. Réputation
    b. Stratégique
    c. Contrôle
    d. Aucune de ces réponses

Test de Connaissances – Q7

7. Quelle catégorie de risques est la plus importante dans le secteur public africain ?
   a. Financier
   b. Opérationnel
   c. Réputation
   d. Aucune de ces réponses

Test de Connaissances – Q8

8. Décider quel niveau de risque est acceptable ou inacceptable considérant chaque catégorie de risques, est une responsabilité clé de:
   a. La Direction
   b. Des auditeurs internes
   c. a et b
   d. Aucune de ces réponses

Test de Connaissances – Q9

9. Les risques sont évalués en termes de:
   a. Vulnérabilité
   b. Impact
   c. Probabilité
   d. a, b, et c

Test de Connaissances – Q10

10. Lequel n'est pas un élément du cadre COSO:
    a. environnement de contrôle
    b. Leadership
    c. Les activités de contrôle
    d. Information et communication

Test de Connaissances – Q11

11. En ce qui concerne les auditeurs internes, quelle phrase est exacte:
    a. L'indépendance est une condition préalable à l'objectivité
    b. L'objectivité est une condition préalable à l'indépendance
    c. L'indépendance et objectivité ne sont pas liées
    d. Les auditeurs internes ne sont tenus d'être objectifs

Test de Connaissances – Q12

12. Dans un contexte de management et d'audit interne fondés sur les risques, recommander des moyens pour éliminer ou réduire les excès de contrôle des risques mineurs est une responsabilité :
    a) De la direction
    b) Des auditeurs externes
    c) Des auditeurs internes
    d) Aucune de ces réponses

Test de Connaissances – Q13

13. Dans le contexte du management et de l'audit interne basés sur le risque, le risque inhérent est normalement évalué en termes de :
    a. Probabilité
    b. Impact
    c. Probabilité x Impact
    d. Dommage financier seulement

Test de Connaissances – Q14

14. Dans un contexte management et d'audit interne basés sur le risque, la cartographie ou Heatmap est une manière de décrire:
    a. Une exposition aux risques
    b. Les risques opérationnels
    c. Les niveaux des critères de risques
    d. Aucune de ces réponses

Test de Connaissances – Q15

15. Lorsque le plan d'audit interne basé sur les risques est complété, dans quel ordre de priorité le chef du département d'audit interne devrait-il communiquer les questions suivantes à la direction:
    I. Détection des expositions aux risques inacceptables
    II. Les principaux objectifs d'audit interne à aborder
    III. les principaux processus de contrôle liés à des objectifs essentiels d'audit
    IV. Les missions d'audit interne exclues du plan de travail annuel
    a. I, II, III, IV
    b. II, III, I, IV
    c. I, III, II, IV
    d. IV, I, II, III

Test de Connaissances – Q16

16. Les objectifs d'audit interne sont principalement liés:
    a. Aux objectifs de gestion du ministère
    b. Aux missions d'audit interne individuelles
    c. Les deux a. et b.
    d. Aucune de ces réponses

Test de Connaissances – Q17

17. Une réunion d'ouverture avec la direction est la suivante:
    a. Obligatoire
    b. Hautement souhaitable
    c. Pas nécessaire
    d. Il vaut mieux éviter d'avoir cette séance d'ouverture pour assurer que l'équipe d'audit interne reste indépendant

Test de Connaissances – Q18

18. En suivant une approche fondée sur le risque pendant une mission d'audit interne, quelle séquence de tâches devraient suivre les auditeurs internes:
    I. Comprendre les objectifs de gestion de l'entité auditée
    II. Comprendre et évaluer les risques de l'entité auditée
    III. Suggérer des possibilités d'améliorations significatives dans l'entité auditée
    IV. Confirmer l'efficacité des pratiques de la gestion des risques et des processus dans l'entité auditée
    a. I, II, III, IV
    b. III, I, II, IV
    c. I, II, IV, III
    d. I, III, II, IV

Test de Connaissances – Q19

19. Quelle est la relation entre les objectifs des missions d'audit interne et les objectifs de l'organisation :
    a. Il n'y a pas de relation
    b. Les objectifs de la mission doivent être liés aux objectifs de gestion
    c. Les objectifs de gestion devraient être liés aux objectifs de l'engagement
    d. Les objectifs de la mission et les objectifs de l'organisation doivent être tous liés aux contrôles internes

Test de Connaissances – Q20

20. Si la direction n'établit pas suffisamment de critères de mesure pour déterminer l'atteinte des objectifs de gestion, les auditeurs internes devraient:
    a. Utiliser leurs propres normes
    b. Délivrer un rapport d'audit interne notant l'absence de critères de mesures adéquats
    c. Travailler avec la direction pour l'élaboration de critères appropriés
    d. Aucune de ces réponses

METHODOLOGIE ET OUTILS D'ELABORATION DE LA CARTOGRAPHIE, DU PLAN DE MITIGATION ET DU PLAN D'AUDIT BASES SUR LES RISQUES	**Date :**	**Durée**
Séquence 3 : Les applications pratiques de l'évaluation des risques	**Classement : Sq3**	**Rédacteur : SS**
Objectifs	♦ Maîtriser les techniques et les outils d'établissement du plan d'audit ♦ Maîtriser la méthodologie d'élaboration du planning d'audit ♦ Savoir planifier les missions individuelles d'assurance et de conseil ♦ Savoir élaborer la cartographie des risques de fraude	

Déroulement

Exposés :

N° Fiches	Titres / Contenu	Stratégie d'animation
11	Etablissement du plan et du planning d'audit	Exposés et discussions
12	Planification et suivi des actions d'amélioration	Exposés et discussions

FICHE N°11 Etablissement du plan et du planning d'audit

1. Rappel des prescriptions des normes IIA -2020 communication ; 2030 – Gestion des ressources

Le Plan d'audit annuel est issu directement de l'analyse des risques de la structure. Il considère aussi les résultats des travaux des corps de contrôle d'autres Ministères, les travaux de la Cour des Comptes, d'auditeurs externes, des missions de diagnostics et programmes des unités de contrôle qualité et les structures de contrôle interne du Ministère.

Le plan répond aux principes énoncés dans les *Normes internationales pour la pratique professionnelle de l'audit interne* émis par l'Institut d'Audit Interne (IIA) et en particulier:

IIA 2020 – Communication et approbation
Le responsable de l'audit interne doit communiquer aux instances dirigeantes son plan d'audit et ses besoins, pour examen et approbation, ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Le responsable de l'audit interne doit également signaler l'impact de toute limitation de ses ressources.

IIA 2030 – Gestion des ressources
Le responsable de l'audit interne doit veiller à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le plan d'audit approuvé.

Interprétation :
On entend par ressources adéquates, la combinaison de connaissances, savoir-faire et autres compétences nécessaires à la réalisation du plan d'audit. On entend par ressources suffisantes, la quantité de ressources nécessaires à la réalisation du plan d'audit. Les ressources sont mises en œuvre efficacement quand elles sont utilisées de manière à optimiser la réalisation du plan d'audit.

Norme IIA 2060 - Rapports à la Direction Générale et au Conseil
Le responsable de l'audit interne doit rendre compte périodiquement aux instances dirigeantes des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit. Il doit plus particulièrement rendre compte:

- de l'exposition aux risques significatifs (y compris des risques de fraude) et des contrôles correspondants ;
- des sujets relatifs au gouvernement d'entreprise; et
- de tout autre problème répondant à un besoin ou à une demande des instances dirigeantes.

2. Le plan pluriannuel et le planning d'audit basé sur le risque en 8 étapes

	Tâche / Responsables
1	Le responsable de l'audit interne liste tous les ensembles potentiellement auditables sur la période du plan d'audit. Si l'organisation dispose d'une cartographie des risques, ces ensembles auditables peuvent correspondre à la notion « d'ensembles homogènes » définie précédemment. Ce listing se doit d'être exhaustif, pour cela plusieurs approches permettent de cerner les missions possibles : - Approche par « métier » de l'organisation - Approche par « entité » : filiales, usines, délégations régionales, agences… - Approche processus : audit du processus « achats », du processus « gestion des stocks »… - Ou encore approche thématique : audit de la sécurité, de la communication, de la politique de vente….
2	Un audit mandaté par l'Institution revêt une importance particulière étant donné qu'il se place au sein d'une stratégie globale de l'Institution et doit être priorisé. Les audits demandés par la hiérarchie supérieure peuvent être : - Des audits thématiques (politique sociale…) - Des audits stratégiques ou de performance - Des audits de conformité - Des audits de la fraude Les audits demandés par les autres commendataires (directions opérationnelles ou fonctionnelles….) viennent compléter les demandes de la direction générale. Toutes ces demandes doivent être formalisées. La direction de l'audit interne, à partir de ces différentes sources d'informations, recense l'ensemble des besoins en termes d'ensembles auditables ou univers d'audit (métiers, entités, processus, thématique).
3	La direction de l'audit interne hiérarchise l'ensemble de ces demandes en fonction des risques spécifiques de chacune des entités potentiellement auditables. Pour cela il dispose de plusieurs sources d'informations : - Les résultats d'une cartographie des risques - Les résultats d'une démarche autoévaluation - Les travaux d'un service « risk management » et/ou d'un service « contrôle interne » si l'organisation en dispose - Le suivi des recommandations des missions précédentes Le responsable de l'audit interne en collaboration avec son équipe peut procéder : - L'identification des risques inhérents (typologie et cause) - à une pondération des risques. Cette pondération s'effectue selon plusieurs critères : • à une appréciation quantitative du risque : évaluer le poids de l'entité auditables en fonction de son volume d'activité • Une appréciation quantitative du risque (probabilité x impact sur une échelle de 5 x5 = 25) • Une appréciation à priori de la maturité du contrôle interne existent dans l'entité auditables (Prévention & Protection sur une échelle de 0 à 3) - A une déduction du risque résiduel apparent (faible, moyen, élevé) - La détermination de l'appétence au risque du management - A une identification des modalités de traitement (plan de mitigation et plan d'audit)
4	Avant de sélectionner les entités auditées, la direction de l'audit interne évalue les ressources et les compétences dont elle dispose pour assurer l'exécution du plan d'audit. Eventuellement elle sollicite des moyens supplémentaires auprès de la hiérarchie.
5	En fonction des demandes préalablement hiérarchisées et des capacités du service d'audit interne (effectif du service et compétences), le directeur du service d'audit interne sélectionne les demandes de missions à retenir dans le plan d'audit. Il élabore un projet de plan d'audit. Les missions sont réparties en **missions d'assurance y compris audit de la fraude, et de**

	conseil
6	Lorsque toutes les missions d'audit sont définies et priorisées, le plan d'audit doit être avalisé par la hiérarchie (le Ministre). Un plan d'audit est défini sur une période de 3 à 5 ans **mais est revu annuellement et peut être modifié sous demande expresse de la direction générale (hiérarchie supérieure)**[16]
7	Si le projet de plan d'audit n'est pas validé par la hiérarchie supérieure, celui-ci est revu par le directeur de l'audit en tenant compte des nouvelles priorités fixées par la hiérarchie supérieure (SE, Directeurs opérationnels et Conseil des Ministres) : (étape 3). Si le projet de plan d'audit est validé par la hiérarchie supérieure, le directeur de l'audit établit un plan d'audit définitif.
8	En fonction des disponibilités des auditeurs et des contraintes de temps éventuelles des entités à auditer, le directeur de l'audit établit un planning d'audit précisant : - La date de début et la durée probable de chaque mission - La composition de l'équipe d'audit - La date de remise du rapport aux audités - ….

3. La démarche et les outils détaillés pour l'élaboration du plan pluriannuel et du planning ABR à partir de la cartographie des risques

L'Elaboration du Plan pluriannuel d'Audit Basé sur les Risques à partir de la cartographie des risques

⇨ Construire une matrice comprenant les éléments suivants:

1. Objectifs de gestion
2. Processus/entités auditables
3. Unités/Département responsables
4. Evaluation des risques inhérents (avec justification des facteurs de risque)
5. Evaluation de la qualité des principaux contrôles clefs en place
6. Evaluation des risques résiduels (avec justification des facteurs de risque)
7. Classer les éléments de l'univers d'audit par niveau de risques
8. Appliquer la politique de couverture d'audit
9. Déterminer les audits sur les 3 prochaines années, le champ d'audit et les objectifs d'audit

3.1 La démarche et outil d'élaboration du plan ABR pluriannuel à partir de la cartographie des risques (à partir de l'étape 7)

La construction du plan d'audit à partir de la cartographie des risques se fait généralement au travers de quatre étapes successives.

1. traduire le niveau de risque attribué à l'objet auditable par la cartographie des risques en une fréquence d'audit cohérente ou politique de couverture

☞ **La politique de couverture**

- L'audit est une activité systématique (tout le champ de l'organisation doit être couvert et audité) et périodique (en principe en un maximum de 3 ans).
- Mais le programme triennal doit reposer sur une analyse du risque (la cartographie).

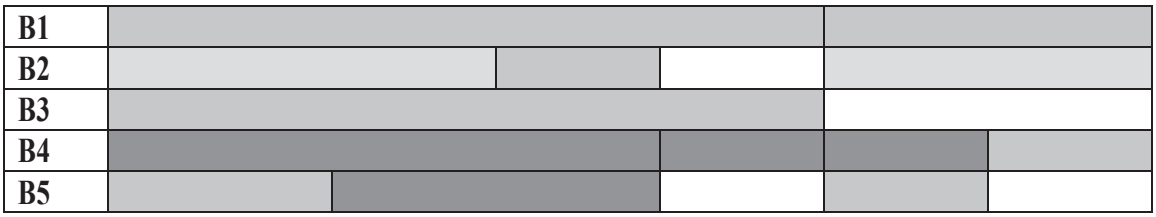
▶Celle-ci **va faire varier la fréquence des missions d'audit selon les différents services qui constituent cette organisation:**

- tous les ans pour les plus exposés (Risques de niveau 1),
- tous les 2 ans pour d'autres, (Risques de niveau 2)
- tous les trois ans seulement, voire rarement, pour les zones de risque faible et accepté (Risques de niveau 3).

[16] Voir ci-après méthodologie de révision ou d'élaboration du plan annuel d'audit en 10 étapes

Chaque institution, à condition d'avoir préalablement effectué ce travail, peut connaître ainsi ***le nombre*** d'auditeurs qui lui sont nécessaires.

Champ de l'Administration à auditer- périodicité



Légende :

L'organisme comporte 5 directions

à auditer tous les ans
à auditer tous les 2 ans
à auditer tous les 3 ans
pourrait être négligé

Nota : A chaque mise à jour du plan d'audit pluriannuel (par exemple en fin d'année), toute modification du niveau de risque issu de la cartographie entraînera ainsi logiquement une révision de la date du prochain audit par rapport au précédent passage, voire un positionnement au plus tôt dans le calendrier de missions en cas de dégradation particulièrement importante et soudaine du niveau de risque.

2. **La deuxième étape dans la construction du plan d'audit est la prise en compte des objets auditables dont le niveau de risque n'a pas été évalué au moyen de la cartographie (cf. point 2 ci-avant).**

Faute de pouvoir disposer comme indiqué ci-dessus d'un niveau de risque issu de la cartographie pour la détermination de la date à laquelle positionner ces objets auditables dans le plan d'audit, **la date sera alors fixée en fonction d'autres critères nécessairement plus subjectifs**. A titre d'exemple, une fonction récemment réorganisé sera souvent auditée dans l'année qui en suit la mise en œuvre, alors qu'une nouvelle activité pourra nécessiter un délai d'un à deux ans avant de pouvoir disposer du recul suffisant pour en effectuer un bilan pertinent.

3. **La troisième étape consiste en l'évaluation des moyens humains nécessaires pour la réalisation des missions positionnées dans le plan d'audit.**

À partir de ce tableau, qui est au fond un plan de charge, on peut déduire ***les besoins*** en nombre d'auditeurs pour effectuer la tâche ainsi définie, **dans le temps imparti et avec la fréquence souhaitée**.

Ce dimensionnement, à la fois quantitatif et qualitatif, sera fonction de différents critères tels que par exemple : la taille des équipes auditées, le niveau de complexité de l'activité ou de l'organisation de l'objet auditable, le besoin de compétences spécifiques en matière technique ou linguistique, le contexte de la mission, etc.

En complément des facteurs énumérés ci-dessus, le niveau de risque issu de la cartographie des risques peut également constituer un bon indicateur pour évaluer le dimensionnement de l'équipe d'audit: les missions sur des objets auditables à risque élevé pourront ainsi être confiées à des auditeurs plus expérimentés et/ou plus nombreux.

4. **Enfin, la dernière étape dans la construction du plan d'audit sera de mettre en cohérence les besoins théoriques déterminés ci-dessus avec les ressources réellement disponibles, tant au niveau quantitatif que qualitatif.**

En cas de déséquilibre important entre les deux, sur une ou plusieurs années du plan pluriannuel, les arbitrages suivants pourront être demandés ou mis en œuvre :

- obtenir des moyens supplémentaires pour la réalisation du plan d'audit;
- reporter certaines missions dans le temps afin de rétablir l'équilibre global entre besoins et ressources, si certaines années du plan sont plus chargées que d'autres du fait des fréquences d'audit retenues;
- revoir ponctuellement le périmètre des travaux prévus, par exemple en retirant du périmètre d'audit une activité ou une direction de l'objet auditable jugée moins risquée que les autres. A noter que ce type d'arbitrage ne saurait être utilisé de façon durable, car il introduit une distorsion entre la vision des risques donnée par la cartographie des risques et celle retenue pour la planification des missions. A terme, il serait donc préférable de revoir le découpage du périmètre d'audit en objets auditables, afin de restaurer une nécessaire cohérence entre la cartographie des risques et le plan d'audit;
- recourir à une sous-traitance externe pour une partie des travaux envisagés. Cette externalisation pourra notamment être réalisée pour les raisons suivantes: besoin de compétences particulières pour l'audit (par exemple des spécialistes en risques, des statisticiens ou des auditeurs informatiques), connaissance spécifique d'un contexte local ou d'une réglementation étrangère, mutualisation des travaux avec d'autres établissements notamment lors des audits « de Place » des prestations de services essentielles externalisées (PSEE), exigence réglementaire locale (cas de l'audit des diligences en matière de lutte anti-blan- d'liment en Espagne, par exemple), etc.

Quelle qu'en soit la raison, le recours à une sous-traitance externe de travaux d'audit suppose toutefois:

- un cadrage des travaux du prestataire, puis un suivi rigoureux de leur réalisation, par l'audit interne. Ce dernier doit en effet s'approprier le diagnostic produit afin de pouvoir ensuite vérifier par lui-même la correcte mise en œuvre des recommandations émises;
- l'existence d'une ligne budgétaire dédiée à ce type de prestations, que l'audit interne pourra utiliser à tout moment en fonction de ses besoins.

3.2 – La structure du plan pluriannuel (voir Réf.17 : Plan triennal d'ABR)

Traditionnellement, et à quelques spécificités près, chaque page du Plan d'audit va se présenter sous la forme d'un tableau à 9 colonnes s'il s'agit d'un Plan sur 5 ans et à 7 colonnes s'il s'agit d'un Plan sur 3 ans

PLAN D'AUDIT (1994-2000)

(Temps passé exprimé
en semaines/auditeurs)

Audit antérieurs		C.R.	Missions d'audit	1996	1997	1998	1999	2000
Année	Temps passé							
			1.- Structures					
1994	3	5	• Service recrutement			3		
1993	17	16	• Service achats	17			17	
1994	15	18	• Service entretien		15			15
1994	2	25	• Service caisse	2		2		2
1995	5	25	• Service publicité		2		5	
			etc.					
			2.- Cycles - Processus					
1994	12	26	• Trésorerie	12		12		12
1993	20	18	• Investissements	20			20	
			etc.					
			3.- Thèmes					
1992	4	12	• Archivage	4				4
1995	12	15	• Contrats			12		
1993	10	15	• Micro-informatique	10			10	
			etc.					
			4.- Audits à la demande	10	10	10	10	10
			Budget temps...	65	30	39	62	53

- **Les 2 premières colonnes rappellent, pour mémoire, les audits antérieurs en indiquant** :
  - l'année du dernier audit,
  - le temps passé pour le réaliser (exprimé en jours/auditeur ou en semaines/auditeur selon le degré de finesse que l'on souhaite obtenir).

Ce rappel permet de prendre en compte les retards (ou avances) antérieurs, de les apprécier par rapport au nouveau coefficient de risque adopté. Il donne également un élément d'information important qui va aider à l'appréciation du temps estimé nécessaire pour les audits à venir.

- **La troisième colonne indique le coefficient de risque retenu (CR)** lequel détermine la fréquence adoptée sur le Plan.

- **La quatrième colonne mentionne les missions d'audit, classés en :**
  - audit des structures,
  - audit des cycles et processus,
  - audit des thèmes.

Nota : On pourrait ajouter les entités auditables (propriétaires, clients, fournisseurs, supports) :**Cinquième colonne**

Plan triennal 2017/2019
Par ensembles homogènes (Univers d'audit)

Audits antérieurs		**Coefficient Risque (CR)**	**Missions d'audit /**	**Entités auditables**	**2017**	**2018**	**2019**
Années	**Temps passé**						
2011							
2012							
2013							
2014							
2015							
2016							
			Missions d'audit à la demande				
				Budget temps			

⧫ Les autres colonnes suivantes permettent de répartir ces audits sur les années à venir selon la fréquence déterminée comme indiqué précédemment **(3 ou 5 ans).**

3.3 – ***Elaboration du planning de réalisation du plan annuel***

Le planning n'est pas le Plan mais il est **élaboré à partir de la première année du Plan** dont il retient les éléments. Il traduit le Plan d'audit en emploi du temps pour chaque auditeur.

⧫ Pour ce faire, 4 étapes sont à respecter :

1. Connaître les périodes d'indisponibilité de chacun: congés - temps de formation, réunions générales - dates de départ et d'arrivée pour les mutations survenant en cours d'année.
2. À partir de ces données, construire les équipes d'audit en affectant les auditeurs aux missions retenues pour eux et en prenant en compte l'enchaînement des missions.
3. Obtenir l'accord des audités sur les périodes retenues pour les missions d'audit.
4. Élaborer l'emploi du temps de chacun.

⧫ On obtient alors un document qui va permettre:

- à chaque auditeur de prévoir et d'organiser son travail et ses déplacements,
- aux responsables d'audit interne d'insérer leur activité dans ce planning,
- et de suivre l'avancement des travaux.

Planning

	Janvier				Février				Mars				Avril				Mai				Juin			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
• Auditeur 1	V	Achats							Entretien								Trésorerie				Archivage			
• Auditeur 2	V	Achats			Formation				Entretien								Trésorerie						Vacances	
• Auditeur 3	V	Achats							Investissement								Micro				Formation			
• Auditeur 4		Achats			Caisse				Investissement								Micro				Contrats			

⧫ Ainsi on constate sur le planning, ci-dessus :

- que l'Audit du service Achats, prévu au Plan, sera réalisé en janvier et au cours de la première semaine de février par les 4 auditeurs,
- que l'Audit du Service Entretien sera assuré par un seul auditeur de la seconde semaine de février à la troisième semaine d'avril, mais qu'un auditeur supplémentaire se joindra à lui du 1 er mars au 8 avril, etc.

⧫ Ce planning doit évidemment être suivi et mis à jour car les retouches sont incessantes et pour des raisons variées :

- mauvaise estimation du temps de travail nécessaire,
- mutations d'auditeurs en dehors des dates prévues,
- formations avancées ou décalées,
- maladies, absences imprévues,
- audits à la demande urgents et non planifiés,
- indisponibilité des audités,
- etc.

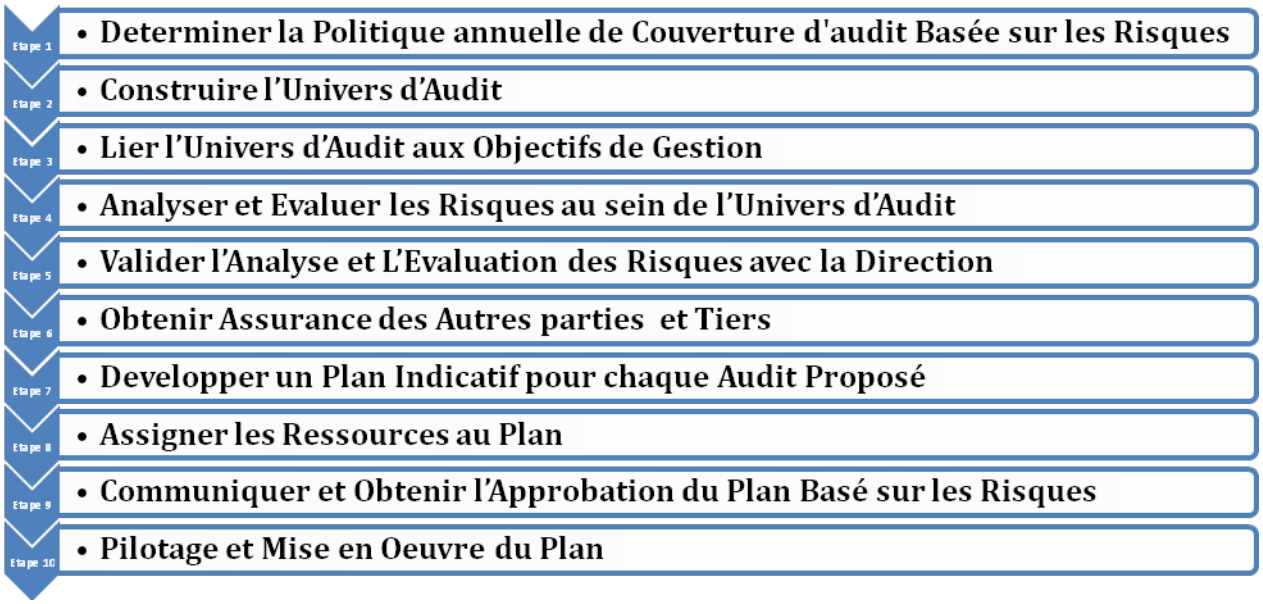
Le suivi des temps de travail s'effectue à partir de relevés de temps réalisés par les auditeurs ou les chefs de mission. Ces relevés permettent l'ajustement permanent du planning : c'est un des rôles essentiels des chefs de mission et du responsable de l'Audit Interne.
Cet ajustement de la réalité sur les prévisions permet l'élaboration du Reporting et des analyses statistiques.

4. Les étapes de la planification annuelle sur la base des risques en 10 Etapes

Le programme annuel est construit sur la base de 10 étapes distinctes.

Les 10 étapes sont les suivantes:

Les Etapes de la Planification Annuelle Basée sur les Risques



❑ Etape 1 : Déterminer la Politique de Couverture Basée sur les Risques

La politique de couverture basée sur les risques s'appuie sur les principes suivants :

1. L'analyse des risques est alignée avec la stratégie de la structure auditée.
2. L'audit concentre son activité annuelle sur :
    a. Les activités/processus où les risques inhérent sont élevés et où l'audit peut apporter une forte valeur ajoutée par son analyse;
    b. Les systèmes de contrôle sur lesquels la structure s'appuie le plus;
    c. Les zones où le différentiel est grand entre risque inhérent et risque résiduel ; et
    d. Les zones où les **risques inhérents sont élevées**.
3. Les zones à risque **inhérent moyen sont examinées selon un cycle triennal**;
4. Les zones **à risque inhérent faible** ne sont pas examinées isolément mais seulement dans le cadre d'audits plus importants.
5. L'audit coordonne ses activités avec les autres corps de contrôle externes et internes.
6. L'évaluation des risques est une activité continue et permanente.
7. Le jugement professionnel est une composante essentielle de l'évaluation des risques.
8. L'évaluation des risques est une démarche participative et transparente du sommet vers la base et de la base vers le sommet.

Autres critères pris en compte dans la politique de couverture : l'importance relative du domaine, l'impact en termes de valeur ajouté, etc.

❑ Etape 2 : Construire l'Univers d'Audit

L'univers d'audit identifie les principaux processus et la responsabilité de chaque structure au sein de la structure. Les processus (gouvernance, métiers, supports) sont le meilleur point d'entrée pour l'analyse des risques et le tableau croisé processus/structures permet de lier les principaux risques à l'ensemble de l'univers d'audit.

- **Etape 3 : Lier l'Univers d'Audit aux Objectifs de Gestion**

Chaque structure se voit confier par les hautes autorités des objectifs opérationnels bien précis : par exemple, réduire la mortalité infantile, augmenter les taux de scolarisation, développer les infrastructures de transport, réduire les inégalités régionales, etc. Il leur revient ensuite d'utiliser les moyens mis à leur disposition pour atteindre ces objectifs dans le respect des quatre contraintes de gestion essentielles à la bonne gouvernance :

- La conformité aux lois et réglementations en vigueur ;
- L'exécution d'opérations éthiques, économiques, efficientes et efficaces ;
- La protection du patrimoine public contre les pertes, les détournements et les dommages ;
- Le respect des obligations de transparence et de compte-rendu démocratique.

- **Etape 4 : Analyser et Evaluer les Risques au sein de l'Univers d'Audit**

Cartographie des risques (projet), (Rapport type élaboration cartographie et plan d'ABR, **Réf. 16 Kit**). Un tableau de hiérarchisation des risques (criticité ou gravité) par processus et par entité est dressé (aux fins de l'élaboration du plan de mitigation).

- **Etape 5 : Valider l'Analyse et L'Evaluation des Risques avec la Direction**

Cette étape intervient par la validation du projet de cartographie des risques avec la haute hiérarchie (les propriétaires), (PV, réunion validation rapport provisoire, Réf.8.3 Kit).

- **Etape 6 : Obtenir Assurance des Autres parties impliquées et Tiers**

Lorsque l'analyse des risques identifie un certain nombre de travaux réalisés par des corps de contrôle d'autres ministères, des travaux réalisés conjointement entre Inspections (particulièrement, l'Inspection Générale des Finances et des inspections techniques sectorielles des ministères) ainsi que la Cour des Comptes, il conviendra de développer cette approche dans le cadre d'une analyse intégrée des risques.

En effet, certains risques systémiques, par exemple ceux liés à la gestion des ressources humaines, systèmes d'information, passation des marchés publics, contrôles de la chaine de la dépense etc. peuvent faire l'objet d'études transversales.

Les bonnes pratiques peuvent être plus facilement disséminées lorsqu'elles s'appuient sur une analyse de la performance des systèmes de gestion. Des faiblesses de contrôle interne communes à plusieurs départements ministériels peuvent faire l'objet de plans d'actions conjoints.

- **Etape 7 : Développer un Plan Indicatif pour chaque Audit Proposé**

En fonction des demandes préalablement hiérarchisées et des capacités du service d'audit interne (effectif du service et compétences), le directeur du service d'audit interne sélectionne les demandes de missions à retenir dans le plan d'audit. Il élabore un projet de plan d'audit.

Les missions sont réparties en **missions d'assurance y compris audit de la fraude, et de conseil**

Assurance et Conseil

Les activités d'audit sont traditionnellement classées selon deux catégories: **assurance ou conseil**. Les missions traditionnelles de l'Inspection comprennent aussi **des investigations** qui sont des missions d'assurance.

Le tableau ci-après identifie les principales différences et caractéristiques des missions d'assurance et de conseil.

Missions d'Assurance: **Les missions d'assurance visent à produire une évaluation objective et indépendante des processus de gouvernance, de gestion des risques et de contrôle en place au sein de l'organisation.**	**Missions de Conseil :** **Ces activités ont pour objectifs d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de gestion. Il s'agit généralement d'études, d'action de formation, facilitation, assistance. Les processus sont généralement en phase de conception, mise en place, transformation et réforme.**
Typologie des missions: ▪ Contrôle de conformité avec politiques et procédures ▪ Architecture du système de contrôle interne ▪ Fonctionnement effectif du système de contrôle interne ▪ Audit de performance ▪ Audit de la fraude Une opinion formelle (par exemple – satisfaisant, à améliorer, non satisfaisant) e**st généralement exprimée sur l'état du système audité**. Une évaluation normalisée de la zone auditée ou de l'importance de chaque constat est généralement fournie (défaillance/faiblesse de contrôle, défaillance/faiblesse significative de contrôle, défaillance/faiblesse matérielle de contrôle).	Typologie des missions : ▪ Avis ▪ Revue de système d'information Pre/ post implémentation ▪ Benchmarking ▪ Formation sur la gestion des risques, le contrôle interne Une opinion formelle n'est généralement pas exprimée.

La répartition du programme entre missions d'assurance et de conseil est fonction de l'analyse des risques, de la maturité de l'organisation en matière de gouvernance, gestion des risques et contrôle; de la compétence professionnelle des auditeurs; de la nécessité de préserver l'indépendance de la fonction d'audit tout en optimisant sa valeur ajoutée.

Chaque audit identifié dans le plan annuel est accompagné d'une description succincte de son objectif et de son périmètre indicatif. Une analyse plus détaillée **et actualisation sera nécessaire lors de la planification individuelle de chaque mission**.

❑ Etape 8 : Assigner les Ressources au Plan (voir tableau d'affectation des ressources, Réf. 18 Kit)

Le plan d'audit annuel a été développé sur une base totale de X jours effectifs d'audit.

Le nombre effectif de jour d'audit (X) est obtenu en considérant les points suivants :

- dans un premier temps, il y a lieu de prendre l'effectif total de la direction de l'audit ;
- ensuite l'audit par les risques devra coexister avec les missions traditionnelles d'investigation spécifiques, exécution de contrôles plutôt qu'opinion sur un système de contrôle ;
- le nombre effectif (indicatif) de jour d'audit correspond à un niveau de contrôle relativement acceptable en considérant par ailleurs qu'il est de bonne pratique en matière de plan basé sur les risques **de conserver 25 à 30%** de temps **non affecté afin de faire face aux risques émergents et missions de conseil décidées en cours d'année et la nécessaire prise en compte d'une courbe d'apprentissage en matière d'audit par les risques** ;

- Il y a lieu enfin de retenir un nombre de journées-hommes du nombre d'auditeurs de la structure d'audit par 200[17] par 75%= X jours d'audit. Ce niveau d'effort doit correspondre à un nombre de missions en considérant qu'une mission de **30 jours est un minimum** en matière d'audit par les risques du fait de normes strictes de documentation des papiers de travail et de toute les étapes de la mission, de la phase de planification, exécution, et enfin de rapportage.

Ce Plan, élaboré une première fois en concertation avec l'équipe d'audit et après consultation des principaux responsables, *doit être ajusté*. En effet, il est nécessaire qu'il y ait **adéquation entre les ressources de l'Audit Interne et les besoins exprimés sur le Plan**.

Le temps disponible pour réaliser des audits est en moyenne de 40 semaines par auditeur et par an. C'est dire qu'une équipe de 3 auditeurs dispose **de 40 x 3 = 120 semaines**.

⧫ Le budget temps figurant dans le Plan d'audit devra donc être adapté à ce chiffre, en prenant deux éléments en considération :

- **1er élément**

Le souhait de la Direction Générale sur l'évolution des effectifs de l'Audit Interne. Ce peut être : croissance, réduction ou maintien.

- **2ème élément**

Quelle que soit l'évolution des effectifs elle ne peut être brutale car il faut sélectionner les auditeurs et **les former** en cas de croissance, se réorganiser en cas de réduction.

⧫ L'élaboration du Plan va donc comporter 5 étapes :

1. Établir (ou mettre à jour) la liste exhaustive des missions d'audit.
2. Calculer (ou mettre à jour) le cœfficient de risque de chaque mission et en déduire la périodicité.
3. Bâtir le projet de Plan après consultation des principaux responsables et l'exprimer en temps/auditeur.
4. Ajuster en fonction des Ressources et des desiderata de la Direction.
5. Faire approuver le Plan par la hiérarchie.

[17] Equivalent de 40 semaines de travail par personne soit 200 jours ouvrable compte tenu des vacances, des maladies, des autres absences justifiées (formations, etc.)

Tableau d'affectation des ressources Réf. 18 Kit

Réf.	*Audit Proposé*	*Type de Revue*	*Effort d'Audit Indicatif (Jours / hommes)*	*Objectifs et Périmètre d'Audit*
A Pilotage ou Gouvernance				
A1	-Audit de conformité -Audit de performance (résultat) -Audit d'efficacité ou de sécurité des Système de Maîtrise des Risques -Audit de la fraude -Audit financier -	Assurance	30 (minimum)	➢ Évaluer l'adéquation de la conception et l'efficacité opérationnelle des contrôles au niveau des entités. Les contrôles au niveau des entités peuvent être, par exemple : • des contrôles sur le risque de contournement par la direction ; • des contrôles sur le processus d'évaluation des risques de l'organisation au niveau de l'entité ; • des contrôles visant à surveiller les résultats des opérations ; • des contrôles sur le processus de communication de l'information financière en fin d'exercice. ➢ Évaluer l'adéquation de la conception et l'efficacité opérationnelle des contrôles des processus métier. Les contrôles des processus peuvent être, par exemple : • des contrôles sur l'efficacité et l'efficience des opérations ; • des contrôles sur la fiabilité de la communication financière et/ou de la direction ; • des contrôles sur la conformité à la législation et à la réglementation applicables. ➢ Évaluer l'adéquation de la conception et l'efficacité opérationnelle des contrôles des systèmes d'information (SI). Les contrôles des SI peuvent par exemple être : • des contrôles généraux au niveau de l'entité tels que les contrôles d'accès au système et les contrôles de gestion des changements; • des contrôles applicatifs intégrés dans les programmes applicatifs spécifiques. ➢ Évaluer directement les performances des processus métier. Les performances des processus peuvent être, par exemple : • l'efficacité et l'efficience opérationnelles exprimées par des indicateurs tels que les • indices de satisfaction des clients, le temps de cycle, la rotation du personnel, etc. ; • la fiabilité de la communication financière, telle qu'exprimée par le nombre et le montant des écritures de correction en fin d'exercice; • la conformité à la législation et à la réglementation applicables, telle qu'exprimée par des indicateurs comme le nombre d'accidents déclarés ou les rejets à l'environnement

A1	- Avis -Etudes -Conseil -Formation	Conseil	30 (minimum)	➢ Exécuter des activités de conseil. par exemple: • des conseils à la direction générale concernant les conséquences pour le risque et les contrôles de la mise en œuvre d'une solution de technologie de l'information avancée; • des conseils aux propriétaires de processus sur la manière de rationaliser ces derniers afin de dégager des gains d'efficience; • des conseils aux managers à tous les niveaux de l'organisation sur la manière de documenter et de regrouper leurs évaluations des risques et des contrôles. ➢ Faciliter les autoévaluations comme ; • l'évaluation par la direction générale des risques qui menacent l'organisation dans son ensemble; • l'évaluation par les propriétaires des processus des risques qui menacent leurs activités. ➢ Mener des formations en interne, par exemple : • renseigner la direction générale sur les nouvelles lignes directrices qui font autorité sur la gouvernance entreprise dans le secteur public, le management des risques et le contrôle ; • informer les propriétaires des processus et le personnel sur les concepts fondamentaux que sont la gouvernance d'entreprise, le management des risques et le contrôle. • Sensibiliser le personnel sur la fraude et la corruption et les contrôles en place pour prévenir et détecter
B Métiers				
B1				
B2				
C Supports ou soutien				
C1				
C2				
	Total			

❑ Etape 9 : Communiquer et Obtenir l'Approbation du Plan Basé sur les Risques par la hiérarchie

Lorsque toutes les missions d'audit sont définies et priorisées, le plan d'audit doit être avalisé par la hiérarchie (le Conseil).Un plan d'audit est défini sur une période de 3 à 5 ans **mais est revu annuellement et peut être modifié sous demande expresse de la direction générale (hiérarchie supérieure).**

La communication doit être exacte, objective, claire, concise, constructive, complète et émise en temps utile. L'identification, **l'évaluation des risques et la détermination des modalités de mitigation font l'objet** :

- d'une validation sur site retenues **(PV compte rendu réunion sur site, Réf. 8.2).**
- d'une validation du rapport provisoire avec la hiérarchie **(PV, réunion validation rapport provisoire, Réf.8.3)**
- d'une prise en compte éventuelle des observations des audités et finalisation du rapport final
- de diffusion du rapport final.

⇨ Sont présents à la réunion de validation du rapport sur la cartographie des risques :

- les auditeurs affectés à la réalisation de la mission,
- la hiérarchie supérieure (propriétaire des risques), accompagné de ses plus proches collaborateurs.

⇨ La réunion de validation a pour finalité de :

- présenter aux audités les conclusions de la mission sous forme de feuilles de risque;
- les valider collectivement avec eux

Lors de cette réunion sont proposés les axes de progrès et un calendrier de mise en œuvre des plans d'action

⇨ **Le projet de rapport est validé techniquement page par page, selon sa structuration :**

- Introduction :
  - rappel des objectifs et des diligences mises en œuvre
  - présentation de façon succincte, des points favorables qui ne donnent pas lieu à des recommandations (points forts)
  - description du système en place
- Analyse des risques : présentation des principaux risques majeurs par processus et des recommandations formulées (modalités de mitigation retenues)
- Plan d'audit basé sur les risques :
  - Présentation de la politique de couverture et du plan d'audit associé
  - Présentation des annexes
    - rappel des concepts-clefs
    - cartographie ou registre des Risques de la structure
    - plan d'Audit Annuel Basé sur les risques de la structure
    - liste des personnes rencontrées
    - documents et rapports consultés
- Plan de management des risques ou de mitigation :
  - Risques
  - Cotation (et rang de priorité)
  - Objectif (Activité/tâche)
  - Action de remédiation (recommandation)
  - Période retenue pour la mise en œuvre
  - Responsable de l'action
  - Coût estimatif

Si le projet de plan d'audit n'est pas validé par la hiérarchie supérieure, celui-ci est revu par le directeur de l'audit en tenant compte des nouvelles priorités fixées par la hiérarchie supérieure (Conseil). Si le projet de plan d'audit est validé par la hiérarchie supérieure, le directeur de l'audit établit un plan d'audit définitif.

Après prise en compte des amendements éventuel des audités, le rapport définitif est formalisé (Réf. 16 Kit).

La CARTOGRAPHIE DES RISQUES est la source principale pour l'identification des besoins d'audit (plan annuel d'audit (Rapport type élaboration cartographie et plan d'ABR, Réf. 16 Kit)).

❑ **Etape 10 : Pilotage et Mise en Œuvre du Plan**

Il est de bonne pratique d'adresser un rapport périodique, au minimum trimestriel à la hiérarchie sur l'exécution du plan (en plus des rapports de mission). Les normes professionnelles de l'audit interne prévoient les dispositions suivantes:

Norme IIA 2060 - Rapports aux Instances dirigeantes
Le responsable de l'audit interne doit rendre compte périodiquement aux Instances Dirigeantes des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit. Il doit plus particulièrement rendre compte:

- de l'exposition aux risques significatifs (y compris des risques de fraude) et des contrôles correspondants;
- des sujets relatifs à la Gouvernance; et
- de tout autre problème répondant à un besoin ou à une demande des Instances Dirigeantes.

5. Les étapes de la planification individuelle de chaque mission et de conduite

5.1 Processus des missions d'assurance

Planifier	Exécuter	communiquer
• Déterminer les objectifs et le périmètre de la mission • Connaître l'audité, notamment ses objectifs et ses assertions • Identifier et évaluer les risques (Tableau des forces et des faiblesses apparentes : voir cartographie ou registre des risques si elle existe) • Identifier les contrôles clés • Evaluer l'adéquation de la conception des contrôles • Etablir un plan de test • Elaborer un programme de travail • Allouer des ressources à la mission	• Réaliser des tests pour collecter des preuves • Evaluer les preuves rassemblées et tirer des conclusions • Elaborer le tableau des forces et des faiblesses réelles • Faire des observations et formuler des recommandations	• Evaluer les observations et faire rencontrer l'information • Procéder à des communications provisoires et préliminaires • Rédiger le rapport d'audit final • Procéder à la communication formelle et informelle des résultats définitifs • Mettre en œuvre des procédures de surveillance et de suivi

5.2 Outils de planification et de réalisation d'une mission d'assurance

Mission assurée par :
Mission supervisée par :

Tableau des risques						Tableau des forces et faiblesses apparentes				Matrice des risques et Contrôles					
Réf.	Finalité / Objectif de CI	Risques potentiel	Points de contrôle ou étapes clefs du CI observables	Impacts	Bonnes pratiques / Moyens du CI, ressources	Force: Contrôles Internes Clefs existants ou adéquats pour mitiger le risque	Faiblesses: Contrôles Internes Clefs manquants ou inadéquats pour mitiger le risque	Commentaires /Justifications / Explications	Evaluation préliminaire des risques (opinion) - Risque Elevé - Risque Moyen - Risque Faible	Evaluation adéquation conception ou Architecture des Contrôles	Résultat du test (Conclusion)	Evaluation de l'Efficacité Opérationnelle des Contrôles Identifiés	Résultat du test (Conclusion)	Conclusion Générale (satisfaisant / à améliorer / non satisfaisant)	Réf. FAR (n/a si non applicable)

FICHE N°12 Planification et suivi des actions d'amélioration

1. Plan d'action (plan de mitigation ou de management des risques)

A la suite de la cartographie, la stratégie de Traitement du Risque (Bonnes pratiques + 4Ts : Traiter, Tolérer, Transférer, Terminer) ou plan de mitigation doit faire l'objet d'un plan d'action proposé par les opérationnels.

⇨ Le plan de mitigation ou de management des risques joint à la cartographie reprend les informations suivantes :

- Risques
- Cotation (et rang de priorité)
- Objectif (Activité/tâche)
- Action de remédiation (recommandation)
- Période retenue pour la mise en œuvre
- Responsable de l'action
- Coût estimatif

Plan de management des risques

Risques	Classement		Objectif (Activité/tâche)	Actions (Recommandation)	Période retenue pour mise en œuvre	Responsable de l'action	Coût estimatif	Indicateur de suivi
	Coef Risque	Rang de priorité						
a	25	1						
b	22	2						

Nota ***: le plan d'action est validé avec le propriétaire du risque (visé par le responsable de l'entité)***

2. La gestion des incidents, rapport et mise à jour du registre des risques

La mise en place d'un système de reporting à la hiérarchie concernée de mise en œuvre du plan de mitigation complète le dispositif.

Le registre des incidents (manuel ou automatisé) donne les indications suivantes :

- risque
- cotation
- propriétaire (responsable de la surveillance)
- sources de données
- méthode de collecte
- Fréquence de la surveillance
- Résultat observé
- Observations

Un reporting périodique sur les incidents est fait à la hiérarchie et à l'audit interne par les responsables des risques (le suivi peut être automatisé).

L'audit interne diligentera également des missions de suivi des missions de suivi de la mise en œuvre des plans d'action de management des risques. Ces actions conjuguées permettent la **mise à jour :**

- des tableaux de bord de suivi des risques,
- et de la cartographie des risques.

Aide-mémoire pour la planification de la mission d'élaboration de la cartographie et l'identification des besoins d'audit

Titres / Contenu	Activités
Projet de planning de réalisation de la mission	A partager
Univers d'audit des cinq (05) Ministères	Elaboration
Répartition des équipes par processus clé retenu et choix des points focaux	Elaboration
Lettre de mission	Complément avec composition des équipes et chronogramme + documentions

Univers d'audit

(A ELABORER)

N°	Structures auditables	Domaines : Processus		
		Gouvernances	Métiers	Supports
1.				
2.				
3.				
4.				
5.				
6.	-			
7.				
8.				
9.				
10.				

Répartition des équipes par processus clé

(A compléter)

N° d'ordre	Chef d'équipe	Membres et adresses	Processus affectés	Point focal désigné par propriétaire des risques
1				
2				
3				
4				
5				
6				

BIBLIOGRAPHIE SOMMAIRE

1. Coopers et Lybrand, IFACI, la pratique du contrôle interne, Editions d'organisation, 2ème édition, 2007
2. Kaplan et Norton, the Balanced Scorecard : Translating Strategy into Action, Boston: HBS Press, 1996
3. Micheal Brassard et Diane Ritter, le Memory Jogger II, GOAL/QPC, The little book of bad excuses, Software program managers network, 1998
4. Jean – Paul Louisot, Gestion des risques, 100 questions pour comprendre et agir, AFNOR Editions, 2005
5. Pascal Kerebel, mise en œuvre d'un contrôle interne efficace via un ERP, AFNOR Editions, 2007
6. Phylippe Noirot, Jacques Walter, 100 questions pour comprendre et agir, le contrôle interne, AFNOR, 2009
7. Alain-Gérard COHEN, Contrôle interne et audit publics, IFACI, LGDJ, 2008
8. Frédéric Bernad, Rémi Gayraud, Laurent Rousseau, Contrôle interne, Maxima, Paris, 2008
9. P. SCHICK, J. VERA, O. BOURROUILH-PAREGE, Audit interne et référentiels de risqué, DUNOD, Paris, 2010
10. Pierre WINICKI, Réussir une réforme publique, DUNOD, Paris, 2007
11. Andre Barilari, Michel Bouvier, La Nouvelle gouvernance financière de l'Etat, LGDJ, 2004
12. Mohamed Hamazaoui, Gestion des risques d'entreprise et contrôle interne, Village Mondiale, Pearson Education France, 2005
13. Sandra Curaba , Yannick Jarlaud , Salvatore Curaba, Evaluation des risques, Comment élaborer son document unique ?, AFNOR, 2009
14. Thierry Malleret, Sean Cleary, Klaus Schwab, Risques - Perception, évaluation, gestion, Maxima Laurent du Mesnil éditeur, 2006
15. The Role of Internal Auditing in Enterprise-wide Risk Management, International Professional Practices Framework Position Paper (Altamonte Springs, FL: The Institute of Internal Auditors. 2009).
16. « La cartographie: un outil de gestion des risques » Ed. AMRAE;
17. IFACI, Price Water house Coopers, Xandwell, Villepele V. (2005), Le management des risques de l'entreprise : Cadre de référence - Techniques d'application, Ed. Organisation ...
18. Cadre de référence de la gestion des risques (2003). FERMA, téléchargeable à l'adresse http://www.amrae.fr/docs/MR/AMRAE/doc-acces-libre/fermacadrereferencerms-french.pdf

ETUDE DE CAS INTRODUCTIF : MANAGEMENT DES RISQUES ET RESPONSABILITE DES GOUVERNANTS

L'Eau à Dakar: Services publics, intérêts privés et choix stratégiques

C'est donc la déchirure d'une pièce en acier intercalée entre deux conduites en fonte qui serait à l'origine de la pénurie sans précédent d'eau potable dans la capitale sénégalaise, selon l'expert Babacar Ndiaye, ingénieur consultant en hydraulique.

"Une défaillance d'ordre technique"

Le serment d'un ingénieur de conception l'oblige à toujours mettre la sécurité du public au cœur de son engagement professionnel. La fiabilité des infrastructures physiques est loin d'être la seule garantie de cet engagement. L'opérationnalisation du système et son adéquation avec la communauté dans laquelle il s'insère sont autant de responsabilités dont l'ingénieur ne saurait se départir.

Toute justification de la faillite d'un ouvrage d'ingénierie, qui représente un risque à la sécurité au public, ne peut être réduite à "une défaillance d'ordre technique", de surcroît trop précipitamment médiatisée comme imprévisible.
Ceci pour dire que les pannes techniques récurrentes sur cette conduite qui ont été enregistrée ces dernières années devait constituer un signal fort de la nécessité d'analyser le système dans son ensemble pour tout acteur consciencieux du domaine.
Maintenant qu'une catastrophe de cette nature peut écorcher un capital politique, on nous annonce des audits techniques, financiers et organisationnels tous azimuts. C'est a posteriori que l'on considère le dédoublement des conduites et la diversification des sources d'approvisionnement "parce que le schéma actuel constitue une menace à la sécurité publique".

De nombreux ministres de l'hydraulique se sont succédé depuis 1996 et aussi depuis 2004, date à laquelle le gouvernement a confirmé la viabilité de l'infrastructure technique, financière et organisationnelle qui existe aujourd'hui.
De tous ces passages, on retient sept avenants consolidant le statu quo du contrat d'affermage Etat-SONES-SDE. Ce partenariat public privé (PPP) a permis d'augmenter de façon significative, les branchements physiques à un système d'adduction d'eau tout en permettant à la SDE de faire des profits dont dépendent le montant des redevances à l'état.

Un système vulnérable

Aujourd'hui, force est de constater la grande vulnérabilité d'un système dont les responsables de la SDE n'ont pas fini de chanter les louanges en le présentant comme modèle. Ils qualifient la catastrophe d'événement exceptionnel. Les techniciens de la SDE se sont probablement dévoués avec ardeur pour "réparer le tuyau" - et c'est certainement la mort dans l'âme qu'ils ont fini par avouer leur incapacité à le faire -mais fondamentalement, ils n'ont jamais eu les moyens techniques et humains de combler la défaillance de tout un système né de mauvaises décisions prises plusieurs années plus tôt.

Il est important de noter que le fait de ne pas prendre de décisions est une décision. Les techniciens donc n'ont que les moyens de maintien du statu quo, pas ceux requis pour faire face à la matérialisation du risque inhérent (et élevé) de la configuration courante du système.

Soit le système n'avait que très peu d'incitatifs à investir des ressources dans le contrôle de ce risque, sachant que ce genre d'investissements nécessite des ressources humaines et techniques sans générer de retours directs sur investissement, soit ce système ne prévoyait pas de possibilité de problèmes majeurs sur une conduite dont la faillite constitue un grand risque au public.
Y a t il défense d'intérêts spécifiques en conflit direct avec l'intérêt du plus grand nombre ou y a-t-il incapacité caractéristique à anticiper et agir dans un environnement en perpétuel mouvement ?

Pourtant, la réussite de toute politique de développement dépend largement de la capacité d'anticiper dans la mesure du possible les mutations constantes du monde. Les experts en eau du pays ont anticipé voilà plus d'une décennie, les exigences nouvelles des citadins modernes en termes de

services publics. Ils ont fourni leurs recommandations aux preneurs de décisions quant à l'extension et au renouvellement du réseau de distribution ainsi qu'à la diversification des sources d'approvisionnement de la capitale sénégalaise. Un constat y alertait déjà les autorités sur la nécessité de bien mobiliser la ressource Eau en amont du réseau de distribution et insistait beaucoup plus sur cet aspect que sur la multiplication de forages, que nous annoncent aujourd'hui les plus hautes autorités du pays.

Les dirigeants de nos pays prennent souvent de bien mauvaises décisions ; cela contribue significativement à la difficulté que nous avons à améliorer notre sort commun.

Des connaissances mal exploitées

La mémoire de l'état est encore mal gérée en ce sens que la conservation des connaissances est mal valorisée. Combien d'études sont redondantes ? Combien de recommandations issues des intelligences vives de la nation pourrissent dans les tiroirs de l'administration ? Un développement soutenu s'appuie en grande partie sur l'encapsulation, la maintenance et la diffusion des connaissances accumulées durant la vie d'une nation. C'est sur cette base que des connaissances nouvelles endogènes peuvent naître et servir. La société sénégalaise regorge de citoyens qui ne manqueront pas de signaler quels événements sont réellement hors de notre portée et quelles sont les conséquences du manque de vision et de prévoyance.
L'intérêt vital de la disponibilité d'eau potable ne se démontre plus dans un contexte d'exode massif vers les villes des pays pauvres.

Pourquoi donc un élément si essentiel à la vie et rare de surcroît devrait-il se payer? La réponse se trouve dans le paradoxe "pénurie d'eau en période d'inondations". Dans le cycle de l'eau, celle-ci coule des montagnes vers les océans via des cours d'eau de surface et des écoulements souterrains. Aucun obstacle ne lui résiste éventuellement. Mais l'ingénierie humaine peut détourner une partie de cette ressource pour la stocker temporairement - dans certaines limites - afin qu'elle soit, entre autres utilisations, distribuée sous forme potable. Ce sont donc les systèmes conçus pour le contrôle relatif de la ressource qui ont un coût, en comparaison à la gratuité d'une dépendance sur la pluviométrie pour les besoins sociétaux liés à l'eau (irrigation, énergie, navigabilité et commerce).

Les choix que font ceux qui ont dépensé de l'énergie pour le privilège de prendre en charge la destinée d'un peuple doivent constamment contenir les risques que leurs décisions impliquent. La vigilance dans la minimisation du risque lié à leurs décisions est capitale.
Il est crucial d'évaluer et de comprendre les conséquences de la défaillance d'un système et de ses composantes.

On ignore la gravité du risque

Les avancées récentes dans la connaissance ont dévoilé aux professionnels du métier, la complexité des systèmes hydriques. Cela a conduit à l'émergence du concept de gestion intégrée de l'eau. Les gestionnaires de l'eau doivent réévaluer régulièrement les systèmes. C'est bien pourquoi la déclaration du directeur de la SDE, disant qu'en 36 ans de métier il n'a jamais vu une panne pareille, ne suffit pas à exempter les personnes en charge, de la responsabilité d'être proactif dans un monde en constante mutation. La maitrise des enjeux, les exigences en quantité et qualité des services publics et les conséquences potentielles d'une rupture d'offre de services ne sont pas les mêmes pour une ville de 300 000 habitants en 1971 versus une ville de 3 000 000 d'habitants en 2013.

Mais pour revenir à l'événement supposément "exceptionnel" que constitue la défaillance d'un tuyau dans un réseau de distribution d'eau potable, un ministre du gouvernement a insisté sur le fait qu'il faudrait au-delà de 6000 camions-citernes en rotation permanente pour pallier à la perte enregistrée du fait de l'incident.
Cela devrait plutôt pousser à réfléchir sur la gravité du risque qui a été ignoré plutôt que sur le manque de moyens a posteriori de faire face à la phase aigüe d'une catastrophe. Trop souvent on dit des calamités qui nous affectent qu'elles sont imprévisibles et au-delà de nos capacités à y faire face: "c'est la volonté divine"! Il y aura toujours des catastrophes dont l'ampleur dépasse les capacités humaines d'anticipation, mais il faudra bien comprendre un jour que cette volonté divine peut être la manifestation de la négligence humaine à prendre consciencieusement ses responsabilités. Cette même volonté divine peut se manifester par la clémence envers ceux qui décident de bien faire les choses pour les bonnes raisons.

Grogne en sourdine

Le gouvernement a annoncé une série de mesures parmi lesquelles le maintien de l'ordre face à ceux qui chercheraient à profiter de la crise pour déstabiliser l'Etat. Il semble que ceux qui souffrent du manque d'eau et d'électricité dans un contexte de chaleur humide et d'inondations n'ont pas besoin qu'on leur suggère leur exaspération. La grogne en sourdine est provoquée par l'offre médiocre, inconstante et chère de services publics sans lesquels les perspectives de vie en société sont sombres. Cette grogne devient de plus en plus facilement exploitable par toute intention organisée.

Le maitre d'ouvrage (l'Etat) a validé - en 1996 - le choix démesurément risqué de faire dépendre une grande partie du transport d'eau potable par une seule conduite. Pire, ce même maitre d'ouvrage n'a pas cru bon de s'assurer de mesures de limitation du risque.
Quelle est la cause des mauvaises décisions impliquant la vie de toute une population? Il peut s'agir du manque de compréhension des enjeux et risques, comme il peut s'agir de décisions délibérées prises sur la base d'un calcul cynique. Dans le deuxième cas de figure, trop souvent il y a un gain personnel - politique ou matériel - et la promotion de privilèges d'une catégorie sociale spécifique qui désormais défendra becs et ongles ses privilèges acquis.

Un certain Mamadou Dia d'un autre temps a compris sur le tard la violente opposition à son action. Sa politique de développement agricole rétablissait un certain équilibre et une certaine justice sociale dans le monde paysan, mais au détriment d'intérêts spéciaux qui jusqu'aujourd'hui plombent la capacité à prendre des décisions propices à un développement économique réel de la nation dans son ensemble. Le tournant qu'a pris le pays depuis se retrouve dans toutes les décisions qui ont conduit à la configuration actuelle de nombreux autres secteurs d'activité économique du pays.
Quand les gouvernants ne développent pas une vision stratégique intrinsèque et cohérente, pour le salut de la société, les projets de développement s'assujettissent assez vite à l'intervention ciblée, sectorielle et fortement conditionnée des bailleurs de fonds. Il arrive que les spécificités techniques des cahiers de charge avantagent considérablement les firmes des pays dont les bailleurs promeuvent les intérêts, même s'ils s'avèrent à l'encontre de l'intérêt public.

Une société française qui poursuit ses propres intérêts

La presse a levé le voile sur un des aspects de cette "catastrophe" programmée: Le bailleur de fonds français a financé la construction de l'usine, dont le contrat a été attribué à une société française.

La société française DEGREMONT aurait donc failli à son devoir de livrer un système techniquement fiable et conforme. Elle serait donc coupable de "fausse déclaration".
Si les conditions d'opération de l'usine n'ont pas outrepassé les limites prescrites par le concepteur de l'usine, c'est vrai. Mais le maitre d'ouvrage a la charge de valider les cahiers de charge et de réceptionner l'ouvrage notamment en en certifiant la conformité avec ses exigences. Il a aussi la charge de veiller sur la pérennité de l'ouvrage.
La société privée DEGREMONT poursuit ses intérêts et cherchera toujours à maximiser ses profits dans le cadre de la marge de manœuvre qui lui est permise. Cela est d'ailleurs vrai de la SDE, société privée aussi, majoritairement française au demeurant et qui défend les intérêts de capitaux privés regroupés au sein du fonds spéculatif Finagestion, semblerait-il.

L'AFD, bailleur de fonds, n'est pas le maitre d'ouvrage et surtout, la responsabilité du maitre d'ouvrage reste entière quant à l'implémentation d'un système de gestion des services publics. Au Rwanda, les bailleurs de fonds s'adaptent à la vision stratégique et aux missions de salut public que ce pays a développé de façon endogène.

Toujours minimiser le risque

La notion de gestion basée sur l'évaluation du risque, issue du paradigme de gestion intégrée des ressources en eau, sied bien aux infrastructures publiques. Il s'agit de toujours minimiser le risque. Cette approche permet de surveiller les maillons faibles du système, de prévoir des mesures avant, pendant et après toute catastrophe.
La SDE, en charge de l'exploitation du réseau, s'est souvent engagée dans une course à l'atteinte d'indicateurs chiffrés, indexée sur le nombre de branchements physiques effectués. Le maitre d'ouvrage doit s'assurer que cette poursuite de branchements "facturables" de la SDE ne se fait pas au détriment

des objectifs réels de la distribution d'eau potable. Dans plusieurs réunions, la SDE s'est félicitée d'être au rendez-vous des objectifs millénaires du développement (OMD) en termes d'accès à l'eau potable. Au-delà des branchements physiques, il est fort possible que ces objectifs soient loin d'être atteints en termes de qualité de l'eau et de sécurisation de l'approvisionnement.
Le maitre d'ouvrage, lui, ne peut se contenter des indicateurs de performances sectoriels au vu de ses responsabilités envers le public. Une vision globale est nécessaire. Pourquoi l'assainissement est-il le parent pauvre du cycle urbain de l'eau devant son parent "riche" alors que dès qu'on touche à l'eau potable, elle devient usée?

Les mauvais réflexes ont la vie dure

Cette crise doit permettre à l'état d'éliminer les incitatifs contre-productifs surtout qu'elle coïncide avec la fin du contrat d'affermage. La faillite du tuyau est donc surtout celle d'un processus de prise de décision et d'un mode de gestion, révélatrice d'une négligence criminelle ou d'une complaisance de compromission tout aussi criminelle. Cette faillite fondamentale est pernicieuse. Elle donne des situations aberrantes dans le domaine de l'énergie, de l'aménagement du territoire, de la téléphonie, voire même de la commercialisation de denrées de première nécessité. Un preneur de décisions peut certes manquer de compétences, disons techniques, mais devrait s'entourer de ceux dont la compétence peut éclairer les enjeux et défis et donc lui suggérer les meilleures décisions possibles pour le salut public.

Il y a encore trop souvent une proportion démesurée de considérations politiques et électoralistes dans les décisions prises.

Malgré l'urgence née hier, les dirigeants doivent prendre les meilleures décisions possibles et pour cela, il faut recourir aux forces vives réellement compétentes, dont le pays ne manque pas. Il faut craindre que les leçons fondamentales ne soient pas encore assimilées. Les mauvais réflexes ont la vie dure, comme en témoigneront les familles des victimes du Joola. A l'époque la mort de plus de 2000 personnes dans le naufrage d'un navire dont la capacité était de 550 personnes avait bouleversé la nation, impuissante devant ses tares systémiques. Cela avait laissé entrevoir la promesse d'une approche disciplinée et consciencieuse de la gestion de la chose publique et du comportement citoyen. Hélas, ce sursaut ne devait durer qu'un printemps.

Alors la question que je pose se trouve dans un texto que je me suis permis d'envoyer à quelqu'un qui fréquente les hautes sphères de la République et que je vous livre en guise de conclusion: "La crise actuelle montre si besoin en est, le rôle central de l'eau dans la vie. Avant que l'amnésie ne nous saisisse, pour peu que l'aspect circonstanciel de la crise ne trouve solution, ne penses-tu pas que les décideurs auraient avantage à prendre conseil chez ceux qui maitrisent réellement les problématiques liés à l'eau?"

Questions :

1. **La situation ci - dessus peut – elle se produire au RDC?**
2. **que vous inspire ce cas réel par rapport au projet de mise en œuvre de l'approche risque dans le secteur public au RDC?**

Cas pratique	Evaluation DES RISQUES	Travaux de groupe de 5

TRAVAUX EN SOUS GROUPE

- **Travail Demandé :**
  - Sur la base de vos connaissances générales votre Ministère et les structures impliquées :

1. Retenez et évaluer 1 risque brut (inhérent) susceptible d'affecter l'atteinte de ces objectifs de gestion (descendre aux activités ou tâches) de la structure retenue :
   - Identifier en groupe les risques potentiels pesant sur les tâches (facteurs d'empêchement internes et externes)
   - Déterminer la catégorie ou typologie de risque (sur 15 types)
   - Imaginer collectivement les causes probables (composant du contrôle interne)
   - Identifier collectivement les conséquences probables de la réalisation du risque
   - Identifiez les responsables impliqués (propriétaire et autres fournisseurs, clients)
   - Évaluer et classer chaque scenario de risque inhérent (probabilité x impact) en appliquant les barèmes de MIRIS
   - Définir l'ensemble des bonnes pratiques de contrôle interne communément admises de maîtrise des risques qui devront exister.
2. Identifiez et évaluez les principaux contrôles internes clés existants liés au risque retenu : Prévention (0 à 3) * Protection (0 à 3)
   - Utilisez votre jugement pour évaluer la maturité des principaux contrôles internes clefs identifiés (utiliser la grille d'évaluation du CI).
3. Evaluez pour le risque retenu, le risque résiduel
   - Déterminez l'Impact Résiduel (IR) = Impact Risque Inhérent – Protection du CI (actions sur les conséquences)
   - Déterminez la Probabilité Résiduel (PR) = Probabilité Risque Inhérent – Prévention du CI (action sur les causes)
   - En déduire le score du risque résiduel = Impact Résiduel x Probabilité Résiduel.
4. Identifier l'appétence au risque du management (niveau A Traiter, Transférer, Tolérer, ou Terminer).
5. Déterminer le niveau de priorisation (échelle de 1 à 3) et classement du risque (déjà survenu : Oui/Non).
6. Elaborez le plan de management du risque (Recommandations, Responsabilité, période pour la mise en œuvre).

- **Votre réponse :**
  - Présentez une réponse écrite aux questions ci-dessus (utilisez l'ordinateur, les résultats seront projetés)
  - Désignez un chef de projet et un rapporteur qui présentera le résultat de vos travaux en plénière.
  - Faire votre présentation en étant prêt à discuter de vos choix avec les autres sous-groupes.

- **Quelques Conseils pour traiter le cas :**
  - Lire le cas attentivement
  - Faire du braingstorming.
  - Suivre les étapes de l'atelier concernant la façon dont vous identifiez, classez les risques, évaluez le risque résiduel (cahier du participant).

Outils à utiliser pour traiter le cas (voir Kit)
Matrice d'évaluation du risque par structure en fichiers Excel
Textes fondateurs de la structure