Cour des comptes
du Canton de Vaud

Audit de la gestion intégrée des risques

Analyse comparative dans cinq entités de l'administration cantonale vaudoise

Projet de rapport n°27

Du 16 décembre 2013

Cour des comptes du Canton de Vaud
Rue Langallerie 11 - 1014 Lausanne
Téléphone : 021 316 58 00 - Fax : 021 316 58 01
Courriel : info.cour-des-comptes@vd.ch

RÉSUMÉ

La notion de risque se définit comme l'effet de l'incertitude sur l'atteinte des objectifs. La gestion des risques se réfère aux pratiques et aux procédures qu'une organisation met en place pour gérer les risques et opportunités auxquels elle est susceptible de faire face. On dit que la gestion des risques est intégrée lorsque l'organisation utilise « une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'organisation d'une manière cohérente et structurée[1] ».

Après un premier audit mené en 2010 dans les musées cantonaux et communaux, la Cour a décidé de conduire une nouvelle mission d'audit sur la vérification de l'évaluation de la gestion des risques dans quatre services de l'Administration vaudoise et au Secrétariat général de l'Ordre judiciaire vaudois, en vertu de la mission qui lui est spécifiquement attribuée par la loi (art. 24 LCC). Selon sa méthodologie[2], la Cour se réfère au modèle COSO II[3] pour évaluer la gestion des risques dans les entités auditées (modèle officiel retenu par INTOSAI[4]).

La Cour des comptes entend, à travers cette mission, encourager et soutenir les entités publiques dans la gestion et la maîtrise de leurs risques. La maîtrise de ceux-ci permet en effet de gérer de façon plus économe, plus efficiente et surtout plus efficace les deniers publics.

Sur le plan du Canton de Vaud, aucune exigence légale en matière d'évaluation des risques ne figure dans les lois et règlements en vigueur.

RÉSULTATS DE L'AUDIT

A travers l'analyse du questionnaire qualitatif, il ressort que, malgré l'absence d'un référentiel de gestion des risques à l'échelle de l'Etat, les entités prennent en compte les risques dans leurs pratiques quotidiennes. Les services audités ont en particulier une maîtrise avérée de leurs risques métiers, c'est-à-dire liés directement aux prestations qu'ils fournissent. Ainsi, les risques identifiés sont-ils essentiellement de type opérationnel.

Les services audités ne disposent cependant pas d'une approche intégrée des risques. La prise en compte des risques est, en général, d'abord pragmatique. Même si certaines procédures sont formalisées, il n'existe pas d'approche systématique en place, telle que celle proposée par le référentiel COSO par exemple (ou d'autres).

[1] Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, 2010.

[2] Manuel de vérification de l'évaluation de la gestion des risques, Méthodologie d'audit de la Cour des comptes du Canton de Vaud, volume 3, septembre 2009.

[3] Enterprise Risk Management – Integrated Framework (Le management des risques de l'entreprise – Cadre de référence), COSO, Septembre 2004. Ce modèle est explicité au chapitre suivant.

[4] Organisation internationales des institutions supérieures de contrôle des finances publiques (INTOSAI GOV 9130, Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public et ses informations complémentaires sur la gestion des risques des entités, ISSAI, 2007).

CONCLUSION

La Cour recommande de mettre en place une gestion intégrée des risques pour l'ensemble de l'administration cantonale vaudoise, qui permettrait aux institutions politiques d'avoir une vision générale des risques majeurs de l'Etat et de disposer ainsi d'un véritable outil de pilotage stratégique, à l'instar de ce qui existe à la Confédération ou dans de nombreuses autres administrations publiques.

L'absence de lignes directrices ou de modèle proposé en matière de gestion intégrée des risques ne permet pas l'éclosion d'une culture du risque partagée au sein de l'Etat. Or, une vision globale est nécessaire pour donner l'impulsion à la mise en place d'une véritable gestion intégrée des risques au niveau stratégique, au-delà de l'approche opérationnelle. Celle-ci doit inclure l'ensemble des risques qui peuvent influer sur la réalisation des objectifs de l'Etat, et partant, sur l'accomplissement de sa mission auprès des citoyens.

Une telle approche peut apporter, en outre, une réelle valeur ajoutée dans le cadre de la mise en place des projets transversaux, notamment décrits dans le programme de législature.

Les constatations et recommandations de la Cour sont présentées dans le tableau ci-après.

REMERCIEMENTS

La Cour rappelle que le présent rapport est destiné à analyser une situation et à informer le public. Il ne saurait interférer ou se substituer à des enquêtes administratives ou pénales.

La Cour formule les réserves d'usage pour le cas où des documents, des éléments ou des faits ne lui auraient pas été communiqués, ou l'auraient été de manière incomplète ou inappropriée, éléments qui auraient pu avoir pour conséquence des constatations et/ou des recommandations inadéquates.

Au terme de ses travaux, la Cour des comptes tient à remercier toutes les personnes qui lui ont permis de réaliser cet audit. Elle souligne la disponibilité de ses interlocuteurs, de même que la diligence et le suivi mis à la préparation et à la fourniture des documents et des données requis.

Ces remerciements s'adressent en particulier à :

- Monsieur Christophe Bornand, chef du Service de protection de la jeunesse
- Madame Sylvie Bula, cheffe du Service pénitentiaire
- Monsieur Pascal Chatagny, chef du Service des automobiles et de la navigation
- Monsieur Steve Maucci, chef du Service de la population
- Monsieur Pierre Schobinger, secrétaire général de l'Ordre judiciaire Vaudois

ainsi qu'à leurs collaboratrices et collaborateurs, pour leur disponibilité et la qualité des échanges.

La Cour remercie également Monsieur Denis Froidevaux, chef du Service de sécurité civile et militaire.

TABLEAU DES CONSTATATIONS ET RECOMMANDATIONS

N°	CONSTATATIONS	RECOMMANDATIONS	PAGE
1	Malgré l'absence d'un référentiel de gestion des risques, les entités prennent en compte les risques dans leurs pratiques quotidiennes. L'approche est pragmatique et principalement orientée métiers.	Dans la perspective d'appréhender et de traiter les risques auxquels l'Etat est confronté dans le développement de ses politiques publiques, les services de l'administration vaudoise devraient disposer des éléments suivants : - un processus de fixation des objectifs à court et moyen terme (SMART) - un inventaire des risques en lien avec les objectifs - une évaluation des risques sur base de l'impact et de l'occurrence, de préférence schématisée dans une cartographie des risques - des plans d'action, qui comprennent la décision de traitement à apporter au risque, avec les activités de contrôle y relatives et le propriétaire du risque - un système d'information et de communication sur la gestion des risques, adapté et efficace - une procédure de suivi et de pilotage du système de gestion des risques.	35-36
2	L'absence de lignes directrices ou de modèle proposé en matière de gestion intégrée des risques ne permet pas l'éclosion d'une culture du risque partagée au sein de l'Etat. Or, une vision globale est nécessaire pour donner l'impulsion à la mise en place d'une véritable gestion intégrée des risques au niveau stratégique, au-delà de l'approche opérationnelle.	La Cour recommande la mise en œuvre d'une gestion intégrée des risques au sein de l'administration cantonale vaudoise. Celle-ci doit inclure l'ensemble des risques qui peuvent influer sur la réalisation des objectifs de l'Etat, notamment ceux figurant dans le programme de législature. Une approche de gestion des risques commune pour l'État de Vaud doit être définie au sein d'une politique de gestion des risques.	37

TABLE DES MATIÈRES

LEXIQUE

Appétence au risque

L'appétence au risque d'une organisation correspond au niveau de risque qu'elle est prête à accepter dans le cadre de sa mission. Elle reflète la philosophie de gestion des risques et influe à son tour sur la culture de l'entité et sa manière d'opérer.

Cartographie des risques

Représentation graphique de l'évaluation des risques dans un tableau à double entrée, l'abscisse représentant la probabilité d'occurrence, et l'ordonnée l'impact estimé du risque.

COSO

Committee of Sponsoring Organizations of the Treadway Commission.

Créée en 1985 pour lutter contre la fraude, le COSO est une initiative conjointe de cinq organisations du secteur privé actives dans le domaine de l'audit et du management, dont le but est d'émettre des référentiels et des lignes directrices en matière de contrôle interne, de gestion des risques et de lutte contre la fraude. Le modèle COSO I traite du contrôle interne, tandis que le modèle COSO II concerne la gestion des risques.

Environnement interne

L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par la direction et l'ensemble des collaborateurs de l'entité. Il dépend notamment du niveau d'engagement de la direction, de l'intégrité et des valeurs éthiques, de la structure organisationnelle et de l'appétence au risque de l'organisation.

Gestion des risques

La gestion des risques se réfère aux pratiques et aux procédures qu'une organisation utilise pour gérer les risques et opportunités auxquels elle est susceptible de devoir faire face. Elle se traduit par « une démarche systématique visant à établir la meilleure façon de procéder dans des circonstances incertaines par la détermination, l'évaluation, la compréhension, le règlement et la communication des questions liées aux risques »[5].

[5] Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, 2010.

Gestion intégrée des risques

La gestion intégrée des risques est « une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'organisation d'une manière cohérente et structurée »[6].

INTOSAI

Organisation internationale des institutions supérieures de contrôle des finances publiques (International Organization of Supreme Audit Institutions).

Risque

Le risque est l'effet de l'incertitude sur l'atteinte des objectifs.

Risque inhérent (ou risque brut)

Le risque inhérent est celui auquel une organisation est confrontée en l'absence de toute action du management susceptible d'influencer sa probabilité de survenance ou son impact.

Risque résiduel

Le risque résiduel est celui qui reste après avoir pris en considération les mesures prises par la direction pour répondre au risque.

Tolérance au risque

La tolérance au risque est le niveau de variation acceptable par l'organisation pour atteindre ses objectifs. Elle dépend de l'appétence au risque de l'organisation, mais se réfère directement aux objectifs.

[6] Idem.

LE CONTEXTE DE L'AUDIT

LA GESTION INTÉGRÉE DES RISQUES

LA DÉFINITION DE LA GESTION DES RISQUES

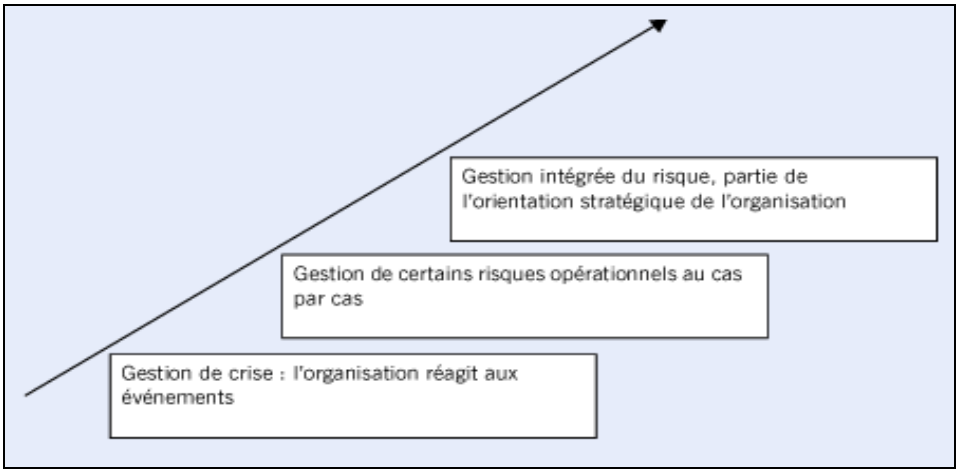
D'abord perçue dans un premier temps comme directement liée à des dangers techniques, la notion de gestion des risques a évolué vers l'analyse des conséquences d'un évènement probable.

Aujourd'hui, la notion de risque se définit de la manière suivante : **le risque est l'effet de l'incertitude sur l'atteinte des objectifs.**

La gestion des risques se réfère aux pratiques et aux procédures qu'une organisation utilise pour gérer les risques et opportunités auxquels elle est susceptible de devoir faire face. Elle se traduit par « une démarche systématique visant à établir la meilleure façon de procéder dans des circonstances incertaines par la détermination, l'évaluation, la compréhension, le règlement et la communication des questions liées aux risques »[7].

DE LA GESTION DE CRISE À UNE GESTION INTÉGRÉE DES RISQUES

La manière de gérer les risques, en particulier la propension de l'organisation à les anticiper, les évaluer et les traiter de manière économe, efficiente et efficace, peut varier beaucoup d'une organisation à l'autre. Le Bureau du Vérificateur Général du Canada identifie trois étapes dans l'évolution progressive de la gestion des risques[8].



[7] Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, 2010.

[8] Rapport de la vérificatrice générale du Canada, chapitre 1 : la gestion intégrée du risques, avril 2003.

La gestion de crise

L'organisation réagit lorsque des évènements surviennent qui ont un impact sur la réalisation de ses objectifs, en ajustant si nécessaire et a postériori les dysfonctionnements constatés. Une gestion des risques basée sur la gestion de crise peut entraîner des coûts importants non prévus et déboucher sur des solutions inefficaces ou inefficientes, sans compter le risque d'image et de discréditation.

La gestion de certains risques opérationnels au cas par cas

L'organisation identifie et évalue ses risques au cas par cas (par exemple, dans le cas d'une nouvelle construction, ou de l'implémentation d'un nouveau programme informatique). La gestion des risques n'est pas intégrée dans un processus global qui tient compte des objectifs de l'organisation et de son appétence au risque[9]. Tous les risques ne sont pas couverts.

La gestion intégrée des risques, partie de l'orientation stratégique de l'organisation

L'organisation utilise « une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'organisation d'une manière cohérente et structurée[10] », dans le but de disposer d'un véritable outil de pilotage stratégique, qui contribue à la réalisation des objectifs globaux de l'organisation, en tenant compte de son appétence au risque.

La gestion intégrée des risques exige une évaluation continue des risques auxquels une organisation peut faire face, à tous les niveaux, ainsi que le regroupement des résultats à l'échelle de l'organisation. Elle permet d'obtenir une vision globale sur l'ensemble des risques et l'interdépendance des composantes, de faciliter l'établissement des priorités et d'améliorer la prise de décisions.

La gestion intégrée des risques doit d'une part, faire partie de la stratégie globale de l'organisation mise en place par le management et, d'autre part, modeler la culture interne de l'organisation autour de la gestion des risques, à tous les niveaux hiérarchiques.

Les organisations qui ne consacrent pas assez d'efforts à l'élaboration d'un cadre pour la gestion intégrée des risques sont susceptibles de n'aboutir qu'à une solution parcellaire : chaque service élabore sa propre solution tant pour la mise en oeuvre du cadre de gestion du risque que pour les façons de réagir au risque. Il en résulte des incohérences au niveau supérieur qui peuvent avoir des conséquences graves sur la vie de l'organisation.

LA GESTION INTÉGRÉE DES RISQUES DANS LE SECTEUR PUBLIC

Le secteur public doit faire face à un environnement toujours plus complexe et à des attentes toujours plus significatives de la part des citoyens et des divers partenaires.

[9] Voir lexique.
[10] Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, 2010.

L'incertitude intrinsèque à la vie de toute organisation est source de risques et d'opportunités, susceptibles de créer ou de détruire de la valeur, ou, dans les termes propres au secteur public, de servir plus ou moins bien l'intérêt public. Ainsi, l'un des principaux défis pour la direction de chaque entité publique réside-t-il dans la détermination d'un degré d'incertitude acceptable afin de garantir la réalisation de sa mission et de ses objectifs et de gagner la confiance des citoyens.

L'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI) a émis des lignes directrices sur la gestion des risques des entités publiques (norme INTOSAI GOV 9130[11]), qui se basent sur le modèle COSO II[12]. La norme GOV 9130 fait partie des normes de bonne gouvernance de l'INTOSAI (INTOSAI GOV[13]) et introduit la gestion des risques de la manière suivante :

« L'entité peut être amenée, en identifiant les risques et opportunités potentiels, à préciser ses objectifs et à élaborer des contrôles internes afin de minimiser les risques et de maximiser les opportunités. La gestion des risques des entités ne suppose pas seulement d'élargir la définition des fonctions englobées dans la gouvernance d'entreprise, mais requiert également un changement dans la manière dont les organisations conçoivent la réalisation de leurs objectifs. Pour être efficace, la gestion des risques des entités représente, en effet, un processus continu pris en compte dans l'élaboration de la stratégie, mis en œuvre à chaque niveau et dans chaque unité de l'organisation et destiné à identifier les évènements potentiels susceptibles d'affecter la capacité de l'organisation à réaliser ses objectifs »[14].

De nombreuses administrations publiques ont mis en place un système de gestion intégrée des risques, dont la Confédération[15], l'Etat de Genève[16], les administrations publiques canadienne[17], française[18] ou encore anglaise[19], pour ne citer que quelques exemples.

Les risques caractéristiques auxquels les organisations publiques sont confrontées sont les suivants :

[11] INTOSAI GOV 9130, Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public et ses informations complémentaires sur la gestion des risques des entités, ISSAI, 2007.

[12] Enterprise Risk Management – Integrated Framework (Le management des risques de l'entreprise – Cadre de référence), COSO, Septembre 2004. Le modèle COSO est également le modèle de référence de la Cour.

[13] L'INTOSAI a émis deux types de normes : les normes ISSAI qui permettent la conduite des audits et les normes INTOSAI GOV consacrées à la bonne gouvernance du secteur public.

[14] INTOSAI GOV 9130, pp. 7-8.

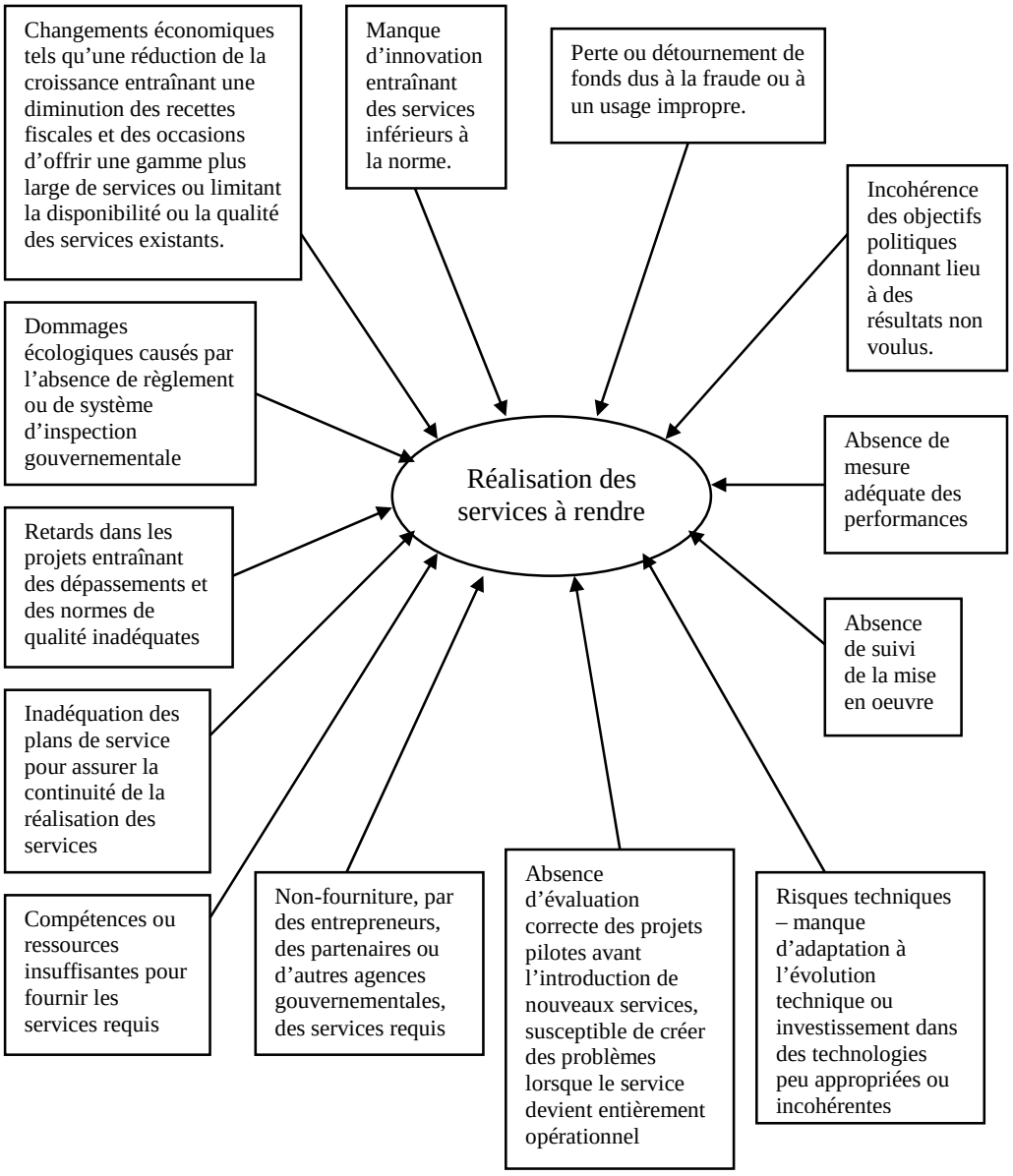
[15] Directives sur la politique de gestion des risques menée par la Confédération du 24 septembre 2010 (Annexe VI) et Politique de gestion des risques de la Confédération, Bases pour la gestion des risques au sein de la Confédération, Département fédéral des finances, décembre 2004 (Annexe VII).

[16] Règlement sur la gestion des risques du 18 septembre 2013.

[17] Guide de la gestion intégrée des risques du Secrétariat du Conseil du Trésor du Canada, 2010

[18] Décret n° 2011-775 du 28 juin 2011 relatif à l'audit interne dans l'administration, Décret n° 2011-497 du 5 mai 2011 relatif au comité stratégique de maîtrise des risques, à la mission d'audit interne et au comité d'audit interne des ministères chargés des affaires sociales.

[19] The Orange Book, Management of Risk - Principles and Concepts, HM Treasury, October 2004.



Source : INTOSAI GOV 9130, Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public et ses informations complémentaires sur la gestion des risques des entités, ISSAI, 2007 », p.16.

LA GESTION INTÉGRÉE DES RISQUES SELON LE MODÈLE COSO

Plusieurs modèles de gestion intégrée des risques existent, dont les plus connus sont notamment ceux développés par le COSO (modèle COSO II), par l'Organisation internationale de normalisation (normes ISO 31000 et 31010) ou encore l'Institut Canadien des Comptables Agréés (modèle CoCo). Le modèle de gestion intégrée du risque qui a été retenu par la Cour est le modèle COSO II, en référence aux normes internationales d'INTOSAI propres au secteur public.

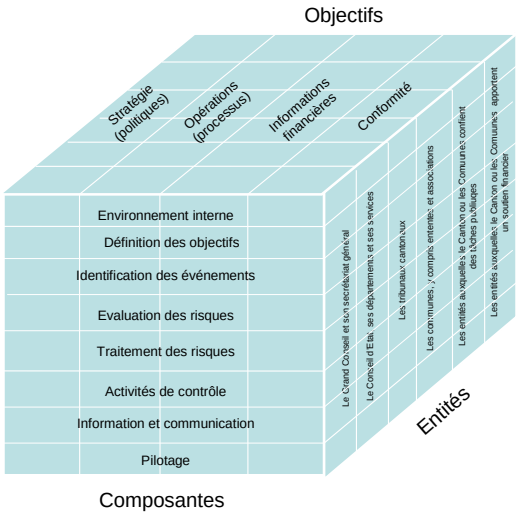
Créé en 1985 pour lutter contre la fraude, le COSO, dont les initiales signifient Committee of Sponsoring Organizations of the Treadway Commission, est une initiative conjointe de cinq

organisations du secteur privé actives dans le domaine de l'audit et du management, dont le but est d'émettre des référentiels et des lignes directrices en matière de contrôle interne, de gestion des risques et de lutte contre la fraude. Le modèle COSO I[20] traite du contrôle interne, tandis que le modèle COSO II concerne la gestion des risques.

Le modèle COSO est représenté sous la forme d'un cube.

Les trois dimensions du cube concernent les éléments suivants :

- les entités concernées
- les objectifs visés
- les composantes de la gestion intégrée des risques.



Les objectifs de la gestion des risques sont regroupés en quatre catégories, qui ont été repris par la Cour des comptes dans sa méthodologie de la vérification de l'évaluation de la gestion des risques[21] :

- les objectifs liés au reporting financier (cette dimension est couverte par le système de contrôle interne)
- les objectifs de conformité (légalité et bonnes pratiques)
- les objectifs opérationnels (économie et efficience)
- les objectifs stratégiques (efficacité des politiques).

Les objectifs stratégiques sont des objectifs de haut niveau, qui reflètent les choix de la direction dans l'accomplissement de la mission de l'organisation. Les objectifs opérationnels, de reporting et de conformité découlent des objectifs définis au niveau stratégique. Les objectifs d'une catégorie peuvent se chevaucher, voire se confondre (par exemple, un reporting spécifique peut à la fois remplir un objectif opérationnel et un objectif de

[20] Le référentiel COSO I vient d'être mis à jour en 2013 (publication prévue en 2014). Sans être une véritable refonte, le nouveau COSO se veut surtout plus agile, en fonction de l'environnement toujours plus complexe dans lequel opèrent les organisations.
[21] Manuel de vérification de l'évaluation de la gestion des risques, Méthodologie d'audit de la Cour des comptes du Canton de Vaud, volume 3, septembre 2009.

conformité, notamment lorsqu'il doit être communiqué dans le cadre d'un reporting externe rendu obligatoire).

La gestion intégrée des risques se décline en huit composantes, qui sont décrites brièvement ci-dessous.

Le Manuel de vérification de l'évaluation de la gestion des risques disponible sur le site internet de la Cour des comptes du Canton de Vaud[22] comporte une description plus complète des diverses composantes.

Les éléments-clés des différentes composantes sont reprises dans un schéma disponible à l'Annexe I.

1. L'environnement interne

L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par la direction et l'ensemble des collaborateurs de l'entité. Il dépend notamment du niveau d'engagement de la direction, de l'intégrité et des valeurs éthiques, de la structure organisationnelle et de l'appétence au risque de l'organisation.

L'appétence au risque d'une organisation correspond au niveau de risque qu'elle est prête à accepter dans le cadre de sa mission. Elle reflète la philosophie de gestion des risques et influe à son tour sur la culture de l'entité et sa manière d'opérer.

Il faut distinguer l'appétence au risque de la tolérance au risque. La tolérance au risque est le niveau de variation acceptable par l'organisation pour atteindre ses objectifs. Elle dépend de l'appétence au risque de l'organisation, mais se réfère directement aux objectifs. Ainsi, l'organisation peut avoir une tolérance zéro par rapport à des objectifs de sécurité, par exemple, mais accepter une marge de 2 % ou de 5 % par rapport à ses objectifs de qualité d'un produit ou de délai dans l'octroi d'un service[23].

2. La définition des objectifs

Les objectifs stratégiques, opérationnels, de reporting et de conformité doivent avoir été préalablement définis pour que le management puisse identifier les évènements potentiels susceptibles d'en affecter la réalisation.

La stratégie ou la façon dont l'organisation va traduire ses objectifs stratégiques en objectifs associés doivent être alignés avec l'appétence au risque de l'organisation. La façon dont elle va mettre en œuvre ses objectifs stratégiques ne doit, ni induire des risques supérieurs à l'appétence de l'organisation pour le risque, ni, à l'inverse, comporter une prise de risque insuffisante pour la réalisation de la mission.

[22] www.vd.ch/autorites/cour-des-comptes/bases-legales.

[23] Une entreprise de transports publics, par exemple, peut avoir l'objectif que tous ses trains arrivent à l'heure. Selon son appétence pour le risque, elle va tolérer un écart de 5 minutes, ou tolérer que 5 % des trains n'arrivent pas à l'heure, ou au contraire avoir une tolérance zéro par rapport à son objectif.

La dimension stratégique est une différence majeure entre le système de gestion des risques (COSO II) et le système de contrôle interne (COSO I). Dans le cadre d'un système de gestion des risques, le processus de fixation des objectifs renforce la cohérence des choix stratégiques de la direction.

L'Annexe II présente un schéma qui illustre la relation entre la mission, les objectifs, l'appétence pour le risque et la tolérance au risque d'une organisation.

Si un dispositif de gestion des risques permet de donner une assurance raisonnable d'atteindre les objectifs de reporting et de conformité, la réalisation des objectifs stratégiques et opérationnels ne dépend pas seulement de l'organisation, mais peut être entravée par des évènements externes. Même si ceux-ci peuvent avoir été prévus dans le cadre de la gestion des risques et fait l'objet d'un plan d'intervention en cas de réalisation, ils échappent néanmoins au contrôle direct de l'organisation.

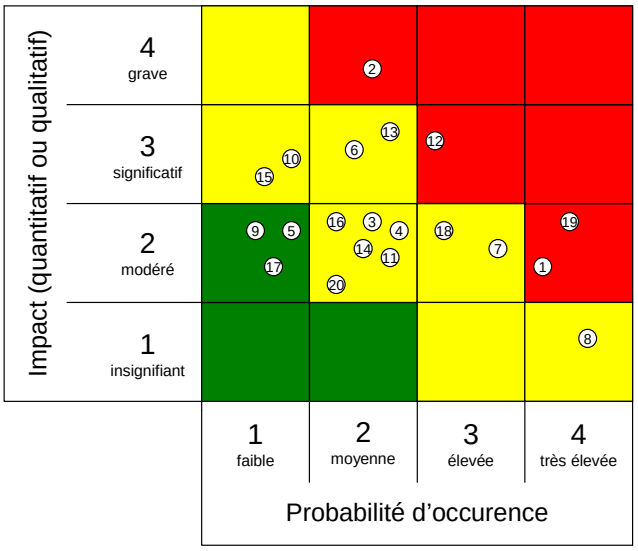
3. L'identification des événements

Les évènements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une organisation doivent être identifiés et documentés dans un inventaire.

4. L'évaluation des risques

L'évaluation des risques permet à l'organisation de fixer ses priorités en matière de gestion des risques. Elle consiste à analyser les risques identifiés, tant en fonction de leur probabilité d'occurrence que de leur impact. La probabilité représente la possibilité qu'un événement survienne au cours d'une période donnée, alors que l'impact désigne l'importance de l'effet que l'événement aura sur la capacité de l'entité à réaliser ses objectifs. Les risques majeurs sont ceux présentant une probabilité de survenance élevée et un impact important. Inversement, les risques faibles sont ceux dont la probabilité de survenance et l'impact sont peu élevés.

Le résultat de l'évaluation des risques est en général schématisé dans un tableau appelé « cartographie des risques ».



Idéalement, l'évaluation doit porter à la fois sur les risques inhérents et sur les risques résiduels.

Le risque inhérent est celui auquel une organisation est confrontée en l'absence de toute action du management susceptible d'influencer sa probabilité de survenance ou son impact.

Le risque résiduel est celui qui reste après avoir pris en considération les mesures prises par la direction pour répondre au risque.

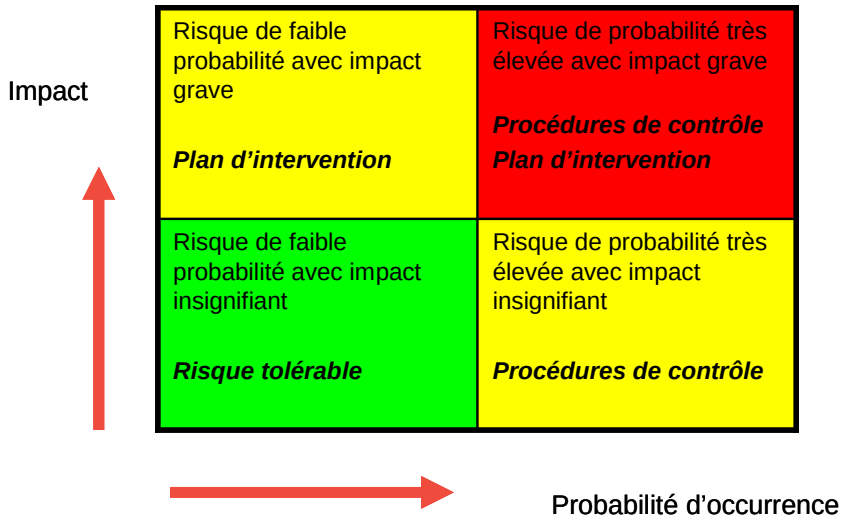
5. Le traitement des risques

Le management définit des solutions permettant de faire face aux risques. Pour ce faire, il élabore un ensemble de mesures permettant de mettre en adéquation le niveau des risques avec l'appétence pour le risque de l'organisation.

Les quatre possibilités d'action face à un risque potentiel sont les suivantes :

- traiter le risque
- transférer le risque
- refuser le risque
- accepter le risque.

Le traitement décidé dépend bien évidemment de l'impact et la probabilité d'occurrence du risque considéré. Les risques faibles peuvent être acceptés. Les risques avec un impact grave, mais une faible probabilité d'occurrence, nécessitent la mise en place de plans d'intervention afin de réduire l'impact en cas de réalisation. L'organisation développera des mesures de contrôle appropriées pour réduire la probabilité d'occurrence des risques avec un impact insignifiant, mais avec forte probabilité de se produire. Dans le cas de risques évalués comme majeurs, l'organisation mettra en place des procédures de contrôle ainsi que des plans d'intervention.



L'objectif d'une gestion intégrée des risques n'est pas de supprimer tout risque, mais de tenter d'en maîtriser ou d'en limiter les effets.

6. Les activités de contrôle

Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques.

7. L'information et la communication

Les informations utiles sont identifiées, collectées et communiquées sous un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'organisation de façon efficace. La communication à l'égard des tiers doit également faire l'objet de procédures précises.

8. Le suivi et le pilotage

Le processus de management des risques est piloté dans sa globalité et modifié en fonction des besoins. Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités.

LA SITUATION DANS LE CANTON DE VAUD

L'ABSENCE D'EXIGENCES (BASE LÉGALE OU RECOMMANDATION)

Sur le plan du Canton de Vaud, aucune exigence légale en matière d'évaluation des risques ne figure dans les lois et règlements en vigueur, ni même de recommandation en la matière.

Toutefois, la Loi sur la Cour des comptes (LCC) mentionne à son article 24, al. b que « la Cour des comptes procède (…) à la vérification de l'évaluation de la gestion des risques des entités soumises à son champ de contrôle ».

Cette attribution est maintenue dans la nouvelle loi sur la cour des comptes du 12 mars 2013, en son article 4.

Considérant que la gestion des risques est un élément clé de la gestion moderne des institutions publiques et conformément à la mission qui lui est confiée par la LCC, cette constatation a fait l'objet d'une recommandation de la Cour des comptes dans le cadre de son audit n° 11 *Evaluation de la gestion des risques dans huit musées cantonaux et communaux* : « La Cour suggère au Canton d'introduire un cadre de référence pour la gestion intégrée de ses risques comme l'a fait notamment la Confédération dès 2004 » (Recommandation n°1).

LES PREMIERS JALONS VERS UNE GESTION INTÉGRÉE DES RISQUES DANS L'ADMINISTRATION VAUDOISE

La Cour relève que l'administration vaudoise a mis en place des projets transversaux qui constituent les premiers jalons d'une évolution vers une gestion intégrée des risques.

Toutefois, en l'absence de cadre de référence, ces projets sont mis en place par des services différents, qui ont une vision par silo, alors que des synergies importantes en termes d'études et de solutions optimisées pourraient être créées.

L'administration vaudoise a pris conscience qu'une gestion de crise n'était plus suffisante, et a pris des initiatives concrètes relativement à la gestion des risques dans les domaines suivants :

La mise en place d'un système de contrôle interne

L'ensemble des services de l'administration vaudoise auront l'obligation, d'ici au 1er janvier 2016, de mettre en place un système de contrôle interne (SCI). Le Département des finances et des relations extérieures a émis en 2010 une nouvelle directive d'exécution n° 22 sur le système de contrôle interne (SCI) et règlement des compétences[24]. Elle fournit un cadre méthodologique pour la gestion des risques liés aux états financiers. Le Contrôle cantonal des finances (CCF) est responsable d'en attester l'existence.

Au 7 mars 2013, sept services de l'Etat ont été certifiés selon la directive 22. Trois autres services ont également débuté la démarche. Le processus a été freiné par la mise en place du

[24] La directive 22 respecte notamment la NAS 890, inspirée directement de COSO I.

nouveau système d'information financier (SAP) et retrouvera un rythme plus soutenu dès que celui-ci sera opérationnel.

La mise en place d'un SCI est une première étape dans la formalisation de la gestion des risques, mais elle se limite dans le canton de Vaud aux risques liés aux états financiers et à certains risques de conformité (principe de légalité en matière de droit financier).

La Politique générale de sécurité des systèmes d'information (PGSSI) et l'analyse des risques de sécurité informatique

Conformément à la Politique générale de sécurité des systèmes d'information (PGSSI, 2011), la Direction des systèmes d'information (DSI) a réalisé une pré-analyse des risques de sécurité informatique dans l'administration cantonale vaudoise. Une cartographie des applications et systèmes critiques a été initialisée afin d'identifier, évaluer et traiter les risques majeurs détectés[25]. Un plan de traitement des risques de sécurité informatique a été élaboré et soumis au Grand Conseil, via un exposé des motifs et projet de décret (EMPD du 17 avril 2013, promulgué le 8 octobre 2013) accordant au Conseil d'Etat un crédit de CHF 8'631'500 destiné à financer la mise en place de mesures de diminution du risque et du pilotage de la sécurité des sytèmes d'information au sein de la DSI.

Il y est notamment mentionné (p. 3) : « *Corriger un ou plusieurs problèmes après leur avènement nuirait très fortement à l'image du service public, le discréditerait et pourrait, suivant la gravité de l'incident, enfreindre la loi sur la protection des données. Pour être proactifs (plutôt que réactifs) et éviter ceci, il faut se donner les moyens de diminuer les risques en identifiant les menaces potentielles ainsi que les vulnérabilités des systèmes pour pouvoir mettre en œuvre un plan de réduction, de transfert ou d'acceptation de ces risques* ».

Cette mesure s'inscrit dans le cadre du Plan directeur cantonal des systèmes d'information 2009-2013 qui vise notamment à optimiser les systèmes d'information au sein de l'Etat, dans un environnement informatique en pleine évolution. Elle s'accompagne en outre de la réalisation de schémas directeurs métiers, qui définissent précisément les processus-clés des entités et mettent en évidence des risques opérationnels liés à l'informatique.

La gestion intégrée des risques naturels

Les diverses catastrophes naturelles survenues durant ces dernières années dans le Canton de Vaud ont incité celui-ci à remettre en cause la politique de gestion des dangers naturels.

La mise en œuvre d'une politique de gestion des dangers et des risques a été confié au Service de la sécurité civile et militaire. Ce mandat a abouti à la publication d'un classeur intitulé « Analyse des dangers et des risques », « véritable outil de réflexion permettant, d'une part, l'établissement au niveau cantonal de plans d'intervention et incitant, d'autre part, les communes à se doter de structures de conduite en cas d'incident majeur »[26]. Les dangers recensés sont regroupés en trois catégories : les dangers naturels, les dangers techniques, les dangers de société.

[25] Rapport annuel de gestion 2012 de l'Etat de Vaud, p. 57.
[26] www.vd.ch/themes/securite/protection-de-la-population/gestion-integree-des-risques

La gestion des catastrophes naturelles et techniques dans le canton de Vaud a fait l'objet d'un rapport de la Cour des comptes[27], qui préconise notamment de définir des objectifs stratégiques en matière de gestion des aléas naturels selon les principes de gestion intégrée des risques recommandés par la Confédération.

[27] Audit de la gestion des catastrophes naturelles et techniques dans le canton de Vaud, rapport n°13 du 7 décembre 2010, Cour des comptes du canton de Vaud.

LA DÉFINITION DE L'AUDIT

LE CHOIX DU THÈME DE L'AUDIT

Après un premier audit mené en 2010 dans les musées cantonaux et communaux, la Cour a décidé de conduire une nouvelle mission d'audit sur la vérification de l'évaluation de la gestion des risques dans quatre services de l'Administration vaudoise et au Secrétariat général de l'Ordre judiciaire vaudois, en vertu de la mission qui lui est spécifiquement attribuée par la loi (art. 24 LCC).

La gestion intégrée des risques vise non seulement à apporter une réponse efficace aux risques et aux opportunités associés aux incertitudes, renforçant ainsi la capacité de l'organisation à réaliser sa mission et ses objectifs, mais aussi à lui permettre de fournir des services plus efficaces, de manière plus efficiente et économique, tout en tenant compte de valeurs telles que l'équité et la justice. La gestion intégrée des risques permet de renforcer la confiance dans l'action publique, en identifiant clairement quels sont les risques et les choix nécessaires.

La gestion intégrée du risque a un rôle à jouer pour rehausser l'efficacité de la fonction publique. Elle contribue à améliorer la gestion et l'exécution des politiques publiques, et à optimiser l'utilisation des ressources. En outre, elle aide les services de l'état à prendre des décisions plus éclairées dans la gestion des risques environnementaux, stratégiques, opérationnels, politiques et financiers qu'ils contrôlent, et elle devrait leur donner de meilleurs moyens d'intervenir face aux risques qu'ils ne contrôlent pas.

La Cour des comptes entend, à travers cette mission, encourager et soutenir les entités publiques dans la gestion et la maîtrise de leurs risques. La maîtrise de ceux-ci permet en effet de gérer de façon plus économe et plus efficiente les deniers publics.

Comme indiqué dans l'Exposé des motifs du projet de loi sur la Cour des comptes (p. 42), la Cour des comptes n'a pas, dans le cadre de ce type de mission, à procéder elle-même à cette évaluation. Ses travaux sont, en revanche, destinés à valider l'existence et à évaluer la pertinence du processus de gestion des risques de l'entité pour les risques de ses activités.

LES OBJECTIFS DE L'AUDIT

Sachant qu'aucune directive en la matière n'est disponible à l'Etat de Vaud, les objectifs de la Cour sont les suivants :

OBJECTIF N°1 : Faire un état des lieux des éléments de gestion intégrée des risques déjà existants au sein de cinq entités de l'administration cantonale vaudoise.

OBJECTIF N° 2 : Apporter une valeur ajoutée relative à la conformité aux bonnes pratiques en matière de gestion intégrée des risques, et par là, améliorer la performance et le dynamisme de la gestion publique.

Les questions d'audit permettant de remplir les objectifs de la Cour sont relatives aux huit composantes du cube COSO II et sont issues de la méthodologie de la Cour spécifique aux audits de vérification de l'évaluation de la gestion des risques[28].

LES ENTITÉS SÉLECTIONNÉES

Les services audités ont été sélectionnés sur la base des critères suivants :

- l'existence d'une culture des risques au sein du service,
- un système de contrôle interne (SCI) certifié conforme à la directive 22 ou en cours d'élaboration.

Par ailleurs, la sélection a tenu compte des services ayant déjà fait l'objet d'un audit de la Cour récemment, ainsi que d'une répartition équitable entre les différents départements (en parallèle avec l'audit sur le risque de corruption).

Les cinq services ci-dessous ont été retenus :

- Le **Secrétariat Général de l'Ordre Judiciaire Vaudois** (SG OJV)
- La **division Asile et Retour du Service de la Population** (SPOP) qui dépend du DECS
- Le **Service des Automobiles** (SAN) qui dépend du DSE
- Le **Service de la Protection de la Jeunesse** (SPJ) qui dépend du DFJC
- Le **Service Pénitentiaire** (SPEN) qui dépend du DINT.

Des informations sur les différents services de l'état de Vaud sont disponibles sur le site www.vd.ch, onglet « Autorités ».

L'APPROCHE D'AUDIT

La Cour a conduit ses travaux conformément à sa méthodologie, en particulier son « Manuel de vérification de l'évaluation de la gestion des risques » (volume 2) et à son « Code de déontologie et Directives relatives à la qualité des audits ». Ceux-ci respectent les normes de contrôle de l'Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques (INTOSAI). En particulier, la Cour s'est référée à la norme INTOSAI GOV 9130, Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public et ses informations complémentaires sur la gestion des risques des entités, qui se base sur le modèle COSO II.

L'équipe d'audit s'est aussi référée aux textes cadres suivants :

- Rapport de la vérificatrice générale du Canada à la Chambre des communes, chap. 1 La gestion intégrée des risques, avril 2003[29].

[28] Manuel de vérification de l'évaluation de la gestion des risques, Méthodologie d'audit de la Cour des comptes du Canton de Vaud, volume 3, septembre 2009.
[29] http/www.oag-bvc.gc.ca

- Guide de la gestion intégrée des risques du Secrétariat du Conseil du Trésor du Canada, 2010[30].
- Directives sur la politique de gestion des risques menée par la Confédération du 24 septembre 2010[31]
- Rapport du Contrôle fédéral des finances : Eidg. Finanzverwaltung Querschnittsprüfung Risikoanalyse auf Stufe Amt und Bund (7 juillet 2008)[32]

L'équipe d'audit était composée de Monsieur Jean-Claude ROCHAT, magistrat responsable, de Madame Anne WEILL-LEVY, magistrate suppléante et de Madame Sandrine NEVEN, cheffe de mandat d'audit, Madame Nathalie Turin , Messieurs Emmanuel Fragnière et Jean Tuberosa, experts.

Pour cet audit en particulier, les démarches ont été les suivantes :

LA COLLECTE ET L'ANALYSE DES INFORMATIONS

Les éléments probants constituant la base sur laquelle reposent les conclusions de l'audit ont été établis en fonction des questions d'audit, dans le cadre des procédures suivantes :

La contribution d'experts

La Cour a mandaté deux experts en les personnes de Messieurs Fragnière et Tuberosa, professeurs à la Haute Ecole de Gestion de Genève, qui ont à leur acquis une longue expérience en matière d'implémentation de système de contrôle interne et/ou de gestion des risques, en particulier dans le secteur public.

Leur approche est pragmatique et véritablement orientée client, ce qui constitue un apport incontestable pour la Cour, dans l'atteinte de ses objectifs.

Monsieur Denis Froidevaux, chef du Service de la sécurité civile et militaire (SSCM), qui représente, entre autres, « l'Autorité cantonale au sens juridique en termes de gestion globale et intégrée des dangers et des risques de toute nature », a également été consulté.

L'élaboration des questionnaires

Pour mener à bien sa mission, la Cour a élaboré deux questionnaires :

- un questionnaire qualitatif qui contient des questions ouvertes sur l'organisation générale du service et sur sa sensibilité par rapport aux risques, permettant à la Cour d'évaluer la première composante d'une gestion intégrée des risques selon le modèle COSO II[33], à savoir l'environnement interne (Annexe III).

[30] http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir01-fra.asp

[31] www.admin.ch/ch/f/ff/2010/5965.pdf

[32] http://www.efk.admin.ch/images/stories/efk_dokumente/publikationen/querschnittspruefungen/QP%20%286%29/8208BE_def_Bericht.pdf

[33] Voir chapitre 1, La gestion intégrée des risques selon le modèle COSO.

- un questionnaire quantitatif qui contient des questions fermées sur l'évaluation du niveau de maturité, au sein de l'entité auditée, de mesures répondant aux sept autres composantes du modèle COSO II (Annexe IV).

Les interviews dans les entités auditées

L'équipe d'audit a consacré une journée dans chacune des entités auditées à interviewer la ou le chef(fe) de service et des membres de la direction.

Afin d'étayer ces questionnaires, les différents interlocuteurs ont fourni certains documents nécessaires pour compléter les informations transmises lors des entretiens.

L'analyse des résultats obtenus

Chacune des huit composantes du modèle COSO a été évaluée spécifiquement sur la base des réponses aux questionnaires, sur une échelle de 1 à 5[34] qui permet d'estimer son degré de maturité. Les chiffres obtenus donnent un indice du degré de maturité de l'évaluation de la gestion des risques dans les entités audités.

Les données obtenues ont été compilées et comparées de manière à obtenir une vision transversale de la gestion des risques au sein des services audités, afin de pouvoir dégager des recommandations de portée générale.

La description détaillée de la méthodologie utilisée pour l'évaluation se trouve au chapitre suivant (Les résultats de l'audit).

LES CONCLUSIONS ET LE RAPPORT

Une fois la collecte et l'analyse des informations probantes finalisées, les constats et recommandations ont été formulés dans une démarche qui se veut constructive afin d'amener une valeur ajoutée.

Le processus a été ensuite celui appliqué à tous les audits de la Cour. Les séances de clôture qui se sont tenues durant le mois d'août ont permis de restituer les conclusions de l'audit et de présenter les recommandations, générales et spécifiques, aux différents services audités.

Le projet de rapport a été approuvé par la Cour le 19 novembre puis adressé aux entités auditées afin que les services puissent formuler leurs observations (délai de 21 jours). Ces observations sont reproduites aux pages 39 à 45 du présent rapport.

Etant donné la portée générale des recommandations, le présent audit a également été envoyé au Chef du Département des Finances et des Relations Extérieures (sa réponse figure à la page 45).

La Cour délibérant en séance plénière en date du 16 décembre 2013 a adopté le présent rapport public en présence de Mme Anne Weill-Lévy, présidente, M. Jean-Claude Rochat, vice-président, Mme Eliane Rey et M. Jacques Guyaz.

[34] L'échelle est définie plus précisément dans le chapitre suivant.

LES RÉSULTATS DE L'AUDIT

Les objectifs du présent audit sont les suivants :

- Objectif 1 : faire un état des lieux des éléments de gestion intégrée des risques déjà existants au sein de cinq entités de l'administration cantonale vaudoise.
- Objectif 2 : apporter une valeur ajoutée relative à la conformité aux bonnes pratiques en matière de gestion intégrée des risques, et par là, améliorer la performance et le dynamisme de la gestion publique.

Pour rappel, la vérification de l'évaluation de la gestion des risques est une des missions de la Cour selon la Loi sur la Cour des comptes (art. 24b).

MÉTHODE D'ÉVALUATION DE LA GESTION DES RISQUES

Pour atteindre ces objectifs, chaque composante du modèle de gestion intégrée des risques COSO II a été évaluée spécifiquement par le biais des questionnaires établis par la Cour (voir Annexes III et IV) et sur base d'un modèle de maturité construit par la Cour (voir Annexe V). Il s'agit des huit composantes suivantes :

1. l'environnement interne
2. la définition des objectifs
3. l'identification des évènements
4. l'évaluation des risques
5. le traitement des risques
6. les activités de contrôle
7. l'information et la communication
8. le suivi et le pilotage

L'évaluation de chaque composante résulte de la moyenne arithmétique des évaluations obtenues à chacune des questions, en référence au modèle de maturité construit par la Cour.

L'évaluation de l'environnement interne a été réalisée a postériori par l'équipe d'audit, sur la base des entretiens semi-directifs avec la direction des entités auditées (questionnaire qualitatif). L'évaluation des autres composantes a été effectuée directement dans l'entité, sur base d'une discussion contradictoire entre la direction de l'entité et l'équipe d'audit[35] (questionnaire quantitatif).

En raison de l'absence de cadre cantonal (contraignant ou même recommandé), la Cour estime pertinent de ne pas individualiser les constatations, le but étant de tirer des constatations de

[35] Pour une des entités dans laquelle l'organisation des visites a été différente, l'évaluation de l'ensemble des composantes a été réalisée a posteriori par l'équipe d'audit, puis soumise à la direction pour validation dans le cadre de la séance de présentation des résultats préliminaires.

portée générale et des recommandations applicables à l'ensemble de l'administration cantonale à partir d'un échantillon observé. Elle a en revanche restitué à chaque service audité les constats et recommandations spécifiques à leur domaine d'activité.

Un modèle de gestion intégrée des risques tel que COSO II suppose que toutes les composantes du modèle soient intégrées dans une logique de management par les risques, soutenue par la direction et concrétisée dans sa politique de gestion des risques.

Ainsi, si les entités auditées ne disposent pas d'une gestion intégrée des risques, elles ont néanmoins, à des degrés divers, mis en place des processus allant dans le sens d'une gestion intégrée des risques, qui méritent d'être valorisés.

Fidèle à son objectif d'apporter une valeur ajoutée en termes de bonnes pratiques, en se basant sur ce qui existe déjà au sein de l'Etat, et dans un souci d'éviter la création d' « usines à gaz », la Cour a évalué chaque composante indépendamment de son intégration dans un système de gestion globale des risques.

Elle a utilisé pour évaluer les éléments de chaque composante une matrice de maturité, basée sur l'échelle d'évaluation suivante :

1- Peu fiable : l'élément considéré est inexistant dans l'organisation.

2- Informel : l'élément considéré existe dans l'organisation, mais de manière informelle et non documentée.

3- Standardisé : l'élément considéré existe dans l'organisation et est formalisé de manière basique.

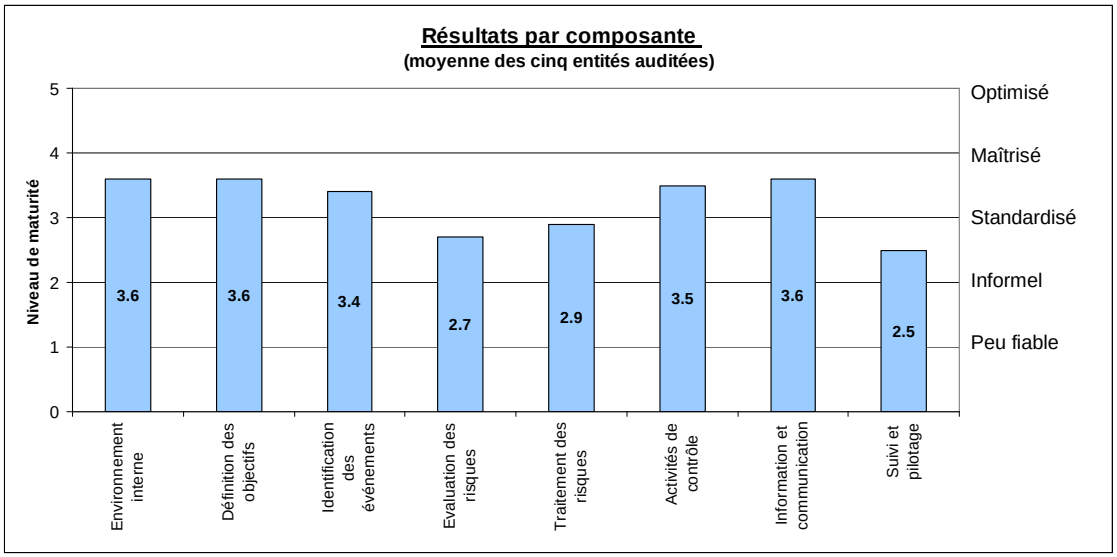
4- Maîtrisé (ou surveillé) : l'élément considéré est développé et documenté dans l'organisation.

5- Optimisé : l'élément considéré est optimisé au sein d'un système de gestion intégrée des risques.

L'évaluation de la composante résulte de la moyenne arithmétique des notes obtenues sur chaque élément considéré.

Le niveau à partir duquel on peut admettre que l'organisation a atteint un degré de maturité considéré comme satisfaisant en l'état actuel, conformément au modèle de maturité développé par la Cour (voir Annexe V) est le niveau 3 – Standardisé.

Les résultats sont les suivants :



Les entités auditées ont obtenu une évaluation allant au-delà du standardisé pour les composantes :

- Environnement interne
- Définition des objectifs
- Identification des évènements
- Activités de contrôle
- Information et communication.

Par contre, elles restent en moyenne au niveau informel pour les composantes :

- Evaluation des risques
- Traitement des risques
- Suivi et pilotage

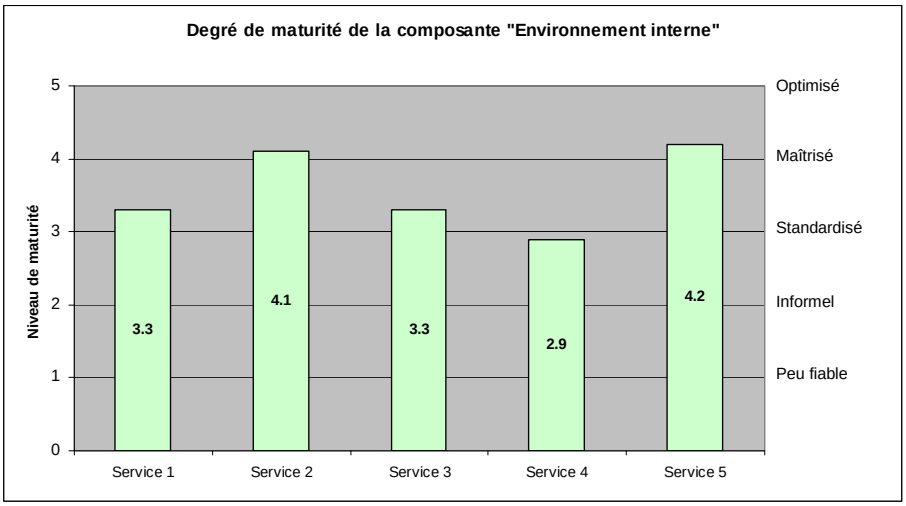
Malgré les bonnes évaluations obtenues pour certaines des composantes prises individuellement, aucune des entités auditées n'a mis en place de système de gestion intégrée des risques. Il existe de bonnes dispositions, mais les risques ne sont pas systématiquement abordés et, en tout cas, pas liés aux objectifs.

L'analyse relative aux huit composantes de la gestion intégrée des risques est présentée ci-dessous. Dans le chapitre suivant, la Cour établit ses constatations, recommandations et conclusion générales.

L'ENVIRONNEMENT INTERNE

L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs. Selon INTOSAI[36], il *constitue le fondement de toutes les autres composantes de la gestion des risques des entités, en fournissant une discipline et une structure* ».

La maturité moyenne de la composante « Environnement interne » des services est évaluée à 3,6 et est présentée pour les cinq services dans le graphique ci-dessous.



LES SERVICES AUDITÉS PRÉSENTENT UNE RÉELLE SENSIBILITÉ AUX RISQUES

La Cour a constaté que la direction des entités auditées témoigne d'une réelle sensibilité aux risques, en particulier les risques métiers auxquels leurs activités les exposent. Les personnes interviewées s'accordent pour dire que l'ensemble de leurs actions et de leurs décisions tiennent compte implicitement des risques encourus. Ils ont à cœur de sensibiliser leurs collaborateurs aux risques.

LA CULTURE ÉTHIQUE EST IMPORTANTE

La mise en place d'une culture éthique propre à son entité demeure une priorité pour les chefs de services audités. Le personnel est régulièrement sensibilisé aux valeurs éthiques du service et on peut parler de « culture d'entreprise » dans la majorité des cas.

Les valeurs éthiques sont mises en avant de manière plus ou moins claire et formalisée dans les services audités. Un seul service s'assure réellement par des actions concrètes et formalisées, que les valeurs éthiques sont connues des collaborateurs et traduites concrètement dans leur métier au quotidien (publication récente d'une charte éthique). Un autre service travaille actuellement sur la formalisation de ses valeurs dans une charte éthique.

[36] Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public – Informations complémentaires sur la gestion des risques des entités, GOV 9130, INTOSAI, 2007, point 2.1.1.

LA GESTION DES RISQUES DOIT ÊTRE INTÉGRÉE ET FORMALISÉE

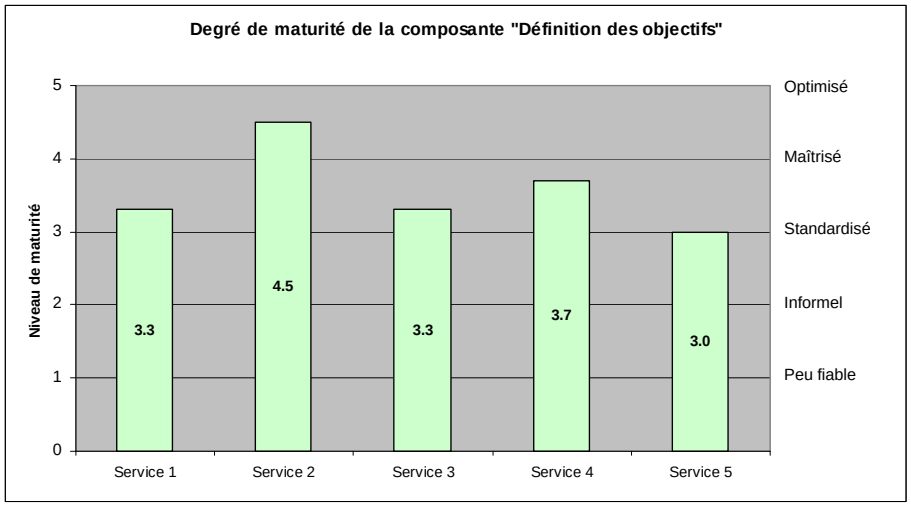
Un système de gestion des risques, tout comme le contrôle interne, nécessite la mise en place de certaines procédures écrites. La formalisation écrite permet d'assurer la transmission et le suivi du savoir-faire et des procédures mises en place. Elle contribue au développement d'un environnement interne sensible au risque. Cette dimension reste à améliorer, de manière générale, dans les entités auditées.

En particulier, les services n'ont pas défini de directive spécifique à la gestion des risques de l'entité. La gestion de certains risques est évoquée dans d'autres politiques internes, comme par exemple, la politique relative à la sécurité, ou la politique relative à la gestion de la qualité, mais l'entité ne dispose pas de vision globale de ses risques et de leur gestion. La politique de gestion des risques permet également de s'assurer que l'ensemble des collaborateurs partage la même appétence au risque[37].

LA DÉFINITION DES OBJECTIFS

La définition des objectifs de l'institution est primordiale en ce sens que le risque est défini par l'effet de l'incertitude sur l'atteinte des objectifs. Il convient donc de définir précisément les objectifs stratégiques, opérationnels, de reporting et de conformité, afin que la direction puisse identifier les évènements potentiels susceptibles d'en affecter la réalisation.

La maturité moyenne de la composante « Définition des objectifs » des services est évaluée à 3,6 et est présentée pour les cinq services dans le graphique ci-dessous.



LA MISSION DES INSTITUTIONS EST DÉFINIE DANS LE CADRE LÉGAL

Les lois et règlements intègrent le plus souvent la description des missions qui incombent à l'Etat. Celles-ci doivent cependant être mises en œuvre à travers des stratégies et traduites en objectifs opérationnels à court (une année) et moyen terme (3 à 5 ans).

[37] Voir lexique.

LES OBJECTIFS ANNUELS SONT FIXÉS EN GÉNÉRAL DANS LE CADRE BUDGÉTAIRE, MAIS NE RÉSULTENT PAS D'UNE PROCÉDURE FORMALISÉE SPÉCIFIQUE (À L'EXCEPTION D'UNE ENTITÉ)

Des objectifs à court terme sont fixés dans les entités auditées, dans le cadre du processus budgétaire. En outre, la procédure d'évaluation du personnel de l'Etat comporte la description des objectifs annuels du collaborateur.

De manière générale, la démarche observée est la suivante : les objectifs politiques sont transcrits en objectifs stratégiques au niveau de la ou du chef(fe) de département et de la direction. Ceux-ci sont ensuite transmis aux chefs de division qui les traduisent en objectifs opérationnels puis personnel pour l'ensemble des collaborateurs.

Dans la plupart des services examinés, la procédure est informelle. De plus, les entités ne s'assurent pas que les objectifs définis soient valides, selon la méthode SMART[38], à savoir qu'ils satisfont aux critères suivants :

- Spécifiques (clairs et précis, sans ambiguïté)
- Mesurables (définis objectivement)
- Accessibles (par ceux qui doivent les atteindre)
- Réalistes (pertinents, s'intégrer dans la logique globale de l'organisation)
- Temporels (qui possède un terme).

Une seule entité dispose d'un vrai système de gestion par objectifs, selon une procédure formalisée. Durant 2 jours, les cadres fixent les objectifs prioritaires du service en se fondant sur divers documents, tels que le rapport annuel, des enquêtes de satisfaction, des rapports d'audits, etc. Une matrice de planification est éditée et communiquée. Trimestriellement, un contrôle est mené par la direction. Un rapport est émis, qui contient l'évaluation de l'état d'atteinte des objectifs (sur une échelle de 3 degrés), mais également des données prévisionnelles (forecast), ainsi que les mesures éventuelles découlant du contrôle. Une à deux fois par année, une synthèse est présentée à l'ensemble du personnel, les objectifs de l'année suivante étant également communiqués à cette occasion.

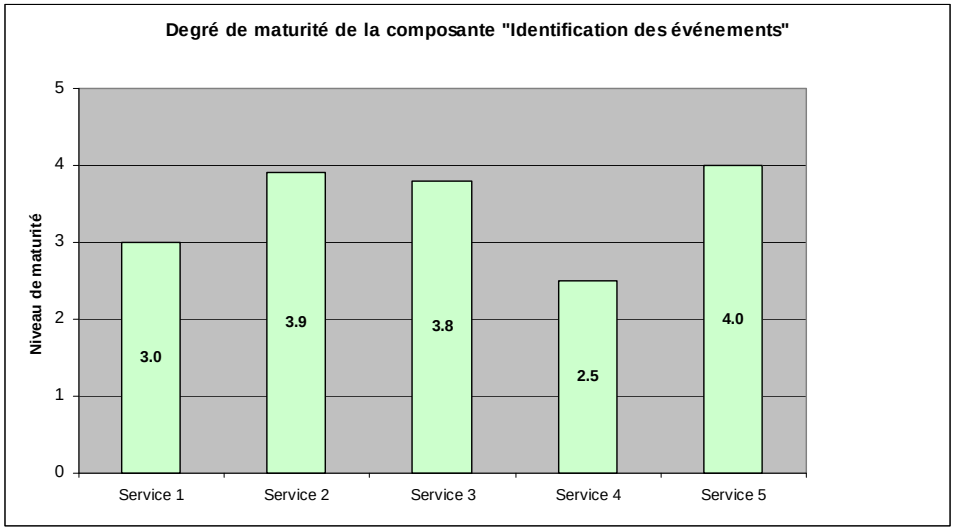
Un autre service pose actuellement les premiers jalons d'une gestion par objectifs.

[38] Repris notamment par la Cour des comptes européenne dans son Manuel d'audit de la performance, les critères SMART permettent de définir des objectifs qui motivent et débouchent sur des résultats concrets et mesurables. La méthode SMART est issue de la Gestion par objectifs, décrite pour la première fois par Peter Drucker en 1954 dans son livre « La Pratique du Management ». Selon Drucker, les dirigeants devraient éviter « le piège de l'activité », étant tellement impliqué dans leurs activités quotidiennes ils en oublient leur objectif principal ou but.

L'IDENTIFICATION DES ÉVÈNEMENTS

Les évènements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une organisation doivent être identifiés dans le cadre d'une procédure spécifique.

La maturité moyenne de la composante « Identification des évènements » des services est évaluée à 3,4 et est présentée pour les cinq services dans le graphique ci-dessous.



LES RISQUES SONT CONNUS MAIS LEUR IDENTIFICATION NE RÉSULTE PAS D'UN PROCESSUS SYSTÉMATIQUE

Les services audités ont une bonne connaissance de leurs risques, même si leur identification ne résulte pas d'un processus systématique. Un certain nombre d'évènements pouvant constituer un risque pour l'entité de ne pas atteindre ses objectifs à court, moyen ou long terme sont identifiés dans le cadre du SCI, de directives ou de manuels divers.

Les aspects financiers sont en général très bien maîtrisés, quatre services sur cinq disposant déjà d'un système de contrôle interne certifié ou en voie finale de certification, impliquant une cartographie des risques financiers. Dans deux services en tout cas, celle-ci intègre également des éléments de conformité. Les délégations des compétences et les règles de signatures sont claires et formalisées.

Les processus dits « métiers », c'est-à-dire relatifs à la gestion opérationnelle et courante des activités, sont décrits dans divers manuels ou directives, voire, pour deux services sous forme schématique au moyen d'un logiciel spécifique. Dans ce cadre, certains risques sont identifiés formellement. Il s'agit au minimum des risques de sécurité, des risques de conformité, voire des risques opérationnels.

L'identification formelle de ces trois types de risques est particulièrement complète dans un service, qui a mis en place un système de gestion de la qualité conformément à la norme ISO 9001.

LES SERVICES NE DISPOSENT PAS D'UN INVENTAIRE DES RISQUES

Bien que leurs risques soient connus, parfois identifiés formellement dans divers documents, les entités ne disposent pas d'une vision globale de leurs risques. Ceux-ci devraient être répertoriés dans un inventaire, en lien avec les objectifs de l'organisation, sur base d'une approche à la fois top-down et bottom-up.

L'IDENTIFICATION DES ÉVÈNEMENTS POUVANT AFFECTER L'ATTEINTE DES OBJECTIFS DES SERVICES DOIT S'INTÉGRER DANS LE CADRE D'UNE GESTION INTÉGRÉE DES RISQUES ET REMONTER AU NIVEAU STRATÉGIQUE

Dans le cadre d'une gestion intégrée des risques, l'identification des risques fait l'objet d'un processus systématique permettant d'identifier les évènements susceptibles d'influencer l'atteinte des objectifs à court, moyen et long terme de l'organisation.

Au-delà des risques financiers, des risques de conformité et des risques opérationnels, l'inventaire devrait également intégrer les risques stratégiques, en accord avec la politique du chef de département et, partant, du Conseil d'Etat.

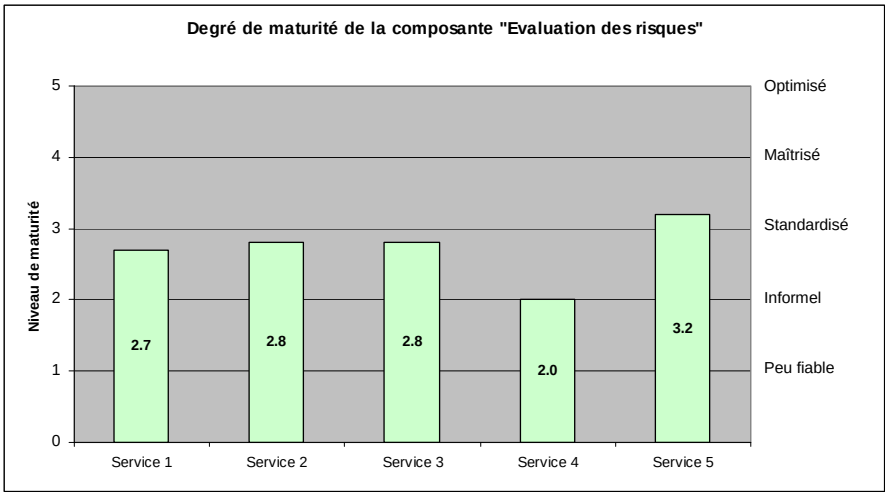
L'ÉVALUATION DES RISQUES

L'évaluation des risques, selon COSO II, implique d'analyser formellement d'une part, l'impact sur l'atteinte des objectifs de l'éventuelle réalisation du risque, d'autre part, sa probabilité d'occurrence. Cette évaluation en termes d'impact et d'occurrence permet de prioriser les risques pour l'organisation, en mettant l'accent sur la gestion des risques majeurs.

L'évaluation des risques est représentée dans une cartographie des risques[39], qui met en évidence la hiérarchisation des risques selon leur impact et leur occurrence, en utilisant les couleurs suivantes : rouges (risques dont l'impact et l'occurrence sont élevés), verts (risques dont l'impact et l'occurrence sont faibles et oranges ou jaunes (risques dont soit l'impact, soit l'occurrence sont élevés).

La maturité moyenne de la composante « Evaluation des risques » des services est évaluée à 2,7 et est présentée pour les cinq services dans le graphique ci-dessous.

[39] Voir chapitre 1, La gestion intégrée des risques selon le modèle COSO, point 4.



LES ENTITÉS N'ÉVALUENT PAS SYSTÉMATIQUEMENT LEURS RISQUES

L'évaluation des risques n'est en général pas systématisée dans les services audités, même si derrière chaque décision, il y a toujours la prise en compte d'un risque. Selon l'expression utilisée par certaines personnes interrogées, l'approche est plutôt « intuitive », basée sur l'expérience et les compétences de la direction et des collaborateurs.

Les quatre services qui disposent déjà d'un système de contrôle interne certifié ou en voie de l'être ont réalisé une évaluation de leurs risques financiers en termes d'impact et d'occurrence.

Un service utilise une méthode reconnue et formalisée pour évaluer un de ses risques opérationnels majeurs.

Dans certains services et pour des projets spécifiques, comme par exemple la construction d'un nouveau bâtiment, une évaluation spécifique des risques a également été menée.

LES SERVICES NE DISPOSENT PAS D'UNE CARTOGRAPHIE DE L'ENSEMBLE DE LEURS RISQUES

En l'absence d'évaluation formelle des risques, les services ne disposent pas d'une cartographie de l'ensemble de leurs risques permettant d'en avoir une vision globale et de les hiérarchiser, selon leur impact et leur probabilité d'occurrence.

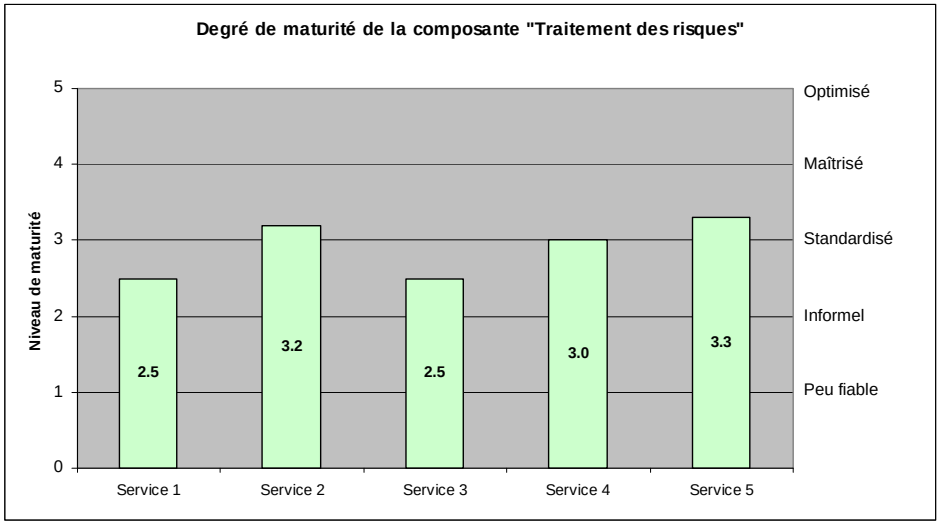
Les services qui ont mis en place un SCI ont toutefois réalisé une cartographie des risques dans le cadre de l'évaluation de leurs risques financiers, voire certains risques de conformité.

Un service a également réalisé une cartographie des risques dans le cadre de la construction d'un nouveau bâtiment (ce service souhaite, à moyen terme, étendre cet exercice à l'ensemble de ses activités).

LE TRAITEMENT DES RISQUES

Pour chaque risque identifié et évalué comme majeur, une réflexion doit être menée quant au traitement le plus approprié à apporter aux risques, selon l'appétence au risque de l'organisation : l'évitement, l'acceptation, la réduction ou le partage du risque.

La maturité moyenne de la composante « Traitement des risques » des services est évaluée à 2,9 et est présentée pour les cinq services dans le graphique ci-dessous.



Les services audités mettent naturellement en place des mesures de traitement de leurs risques : assurances, mesures de sécurité, contrôles internes, etc.

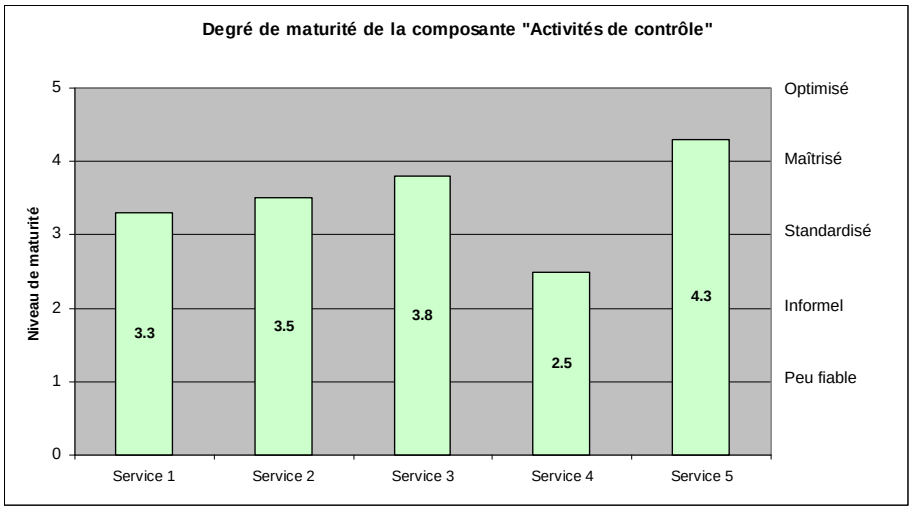
Toutefois, en l'absence de gestion intégrée des risques, les services n'ont pas élaboré de plans d'actions, qui synthétisent les réponses aux risques, en lien avec les objectifs, l'évaluation des risques et leur appétence au risque. De plus, il n'existe pas d'évaluation régulière des réponses aux risques et du risque résiduel, ceux-ci étant réévalués uniquement en cas de dysfonctionnements ou de changements majeurs.

Les plans d'action doivent également désigner, pour chaque risque à traiter, un **propriétaire du risque**, responsable devant la direction de la mise en œuvre du traitement du risque.

LES ACTIVITÉS DE CONTRÔLE

Les activités de contrôle sont axées principalement sur le système de contrôle interne mis en place au sein de l'organisation, afin de garantir que le traitement à apporter aux risques soit réalisé tel qu'il a été décidé.

La maturité moyenne de la composante « Activités de contrôle » des services est évaluée à 3,5 et est présentée pour les cinq services dans le graphique ci-dessous.

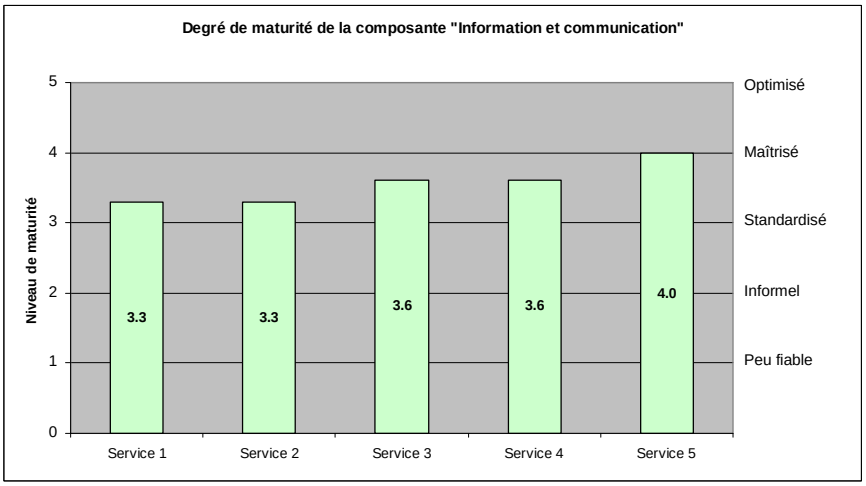


L'ensemble des services ont mis en place diverses procédures de contrôle, en particulier dans le domaine financier et opérationnel, ou encore de la conformité. Toutefois, à nouveau, en l'absence de gestion intégrée des risques, les activités de contrôle ne sont pas intégrées à des plans d'actions, en lien avec les risques et les objectifs.

L'INFORMATION ET LA COMMUNICATION

L'information et la communication sont des éléments essentiels de la gestion intégrée des risques. D'une part, une information dans des formats et des délais adéquats est la garante d'un bon fonctionnement du système, d'autre part une communication tant verticale qu'horizontale est nécessaire afin de véhiculer les valeurs de l'organisation, les objectifs et la gestion des risques.

La maturité moyenne de la composante « Information et communication » des services est évaluée à 3,6 et est présentée pour les cinq services dans le graphique ci-dessous.



IL N'EXISTE PAS DANS LES SERVICES DE SYSTÈMES D'INFORMATION ET DE COMMUNICATION FORMALISÉS DANS LE CADRE D'UNE GESTION INTÉGRÉE DES RISQUES

En l'absence de gestion intégrée des risques, les systèmes de communication et d'information ne sont pas formalisés de manière à garantir la communication, ainsi que la qualité et l'exhaustivité des informations nécessaires au bon fonctionnement du système intégré de gestion des risques. De plus, il s'agit de définir clairement les bases et postulats afin de s'assurer que l'ensemble des parties prenantes parle un langage commun.

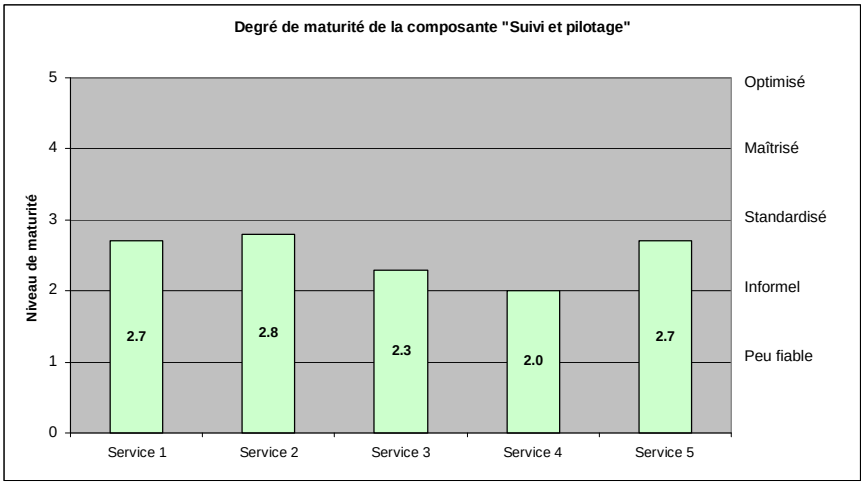
La politique de gestion des risques, l'inventaire des risques, la cartographie des risques et les plans d'actions sont autant d'outils de diffusion de l'information sur le risque.

Toutefois, de manière générale, l'information et la communication fonctionnent bien dans les entités auditées. Trois d'entre elles en particulier font preuve d'une volonté marquée de favoriser la bonne circulation des informations et la communication au sein du service : à titre d'exemple, des réunions sont organisées de manière régulière avec les collaborateurs pour communiquer sur la stratégie et les objectifs de l'entité, des indicateurs sur les résultats du service sont affichés, les valeurs éthiques sont mises en avant, etc.

LE SUIVI ET LE PILOTAGE

Le système de gestion intégrée des risques doit faire l'objet d'un suivi régulier par le management et, le cas échéant, être adapté en fonction des besoins. Le pilotage s'effectue, soit par des contrôles permanents, soit par des évaluations ponctuelles, ou encore par une combinaison de ces deux éléments.

La maturité moyenne de la composante « Suivi et pilotage » des services est évaluée à 2,5 et est présentée pour les cinq services dans le graphique ci-dessous.



Cette composante pourrait être considérée comme non applicable. En effet, puisqu'il n'existe pas de système de gestion intégrée des risques selon COSO II dans les entités auditées, celui-ci ne peut évidemment pas faire l'objet d'un suivi et pilotage.

Néanmoins, la Cour a jugé que le suivi et le pilotage de la gestion des risques dans les entités auditées n'étaient pas inexistants, mais plutôt informels, dans le sens où la direction tient évidemment compte implicitement des risques et de leur évolution pour mener la gestion stratégique de son service.

Il conviendrait, au cas où une gestion intégrée des risques serait mise en place, de définir les moyens de suivi et pilotage à disposition du management et de nommer les responsables des contrôles.

La Cour souligne également l'immense travail réalisé par un service, qui a mis en place un dispositif de pilotage élaboré dans le cadre de l'implémentation d'un système qualité (cockpit qualité).

LES RÉSULTATS PAR ENTITÉ

Pour rappel, en l'absence de cadre légal et afin de ne pas stigmatiser les services, les résultats sont présentés de manière anonyme.

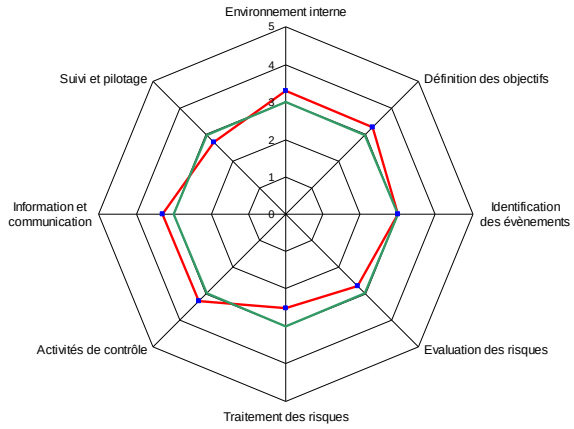
L'analyse menée dans les cinq services fait état de disparités dans le niveau de maturité du système de gestion des risques. Deux causes ressortent de manière plus évidente :

- la spécificité des activités menées par l'entité,

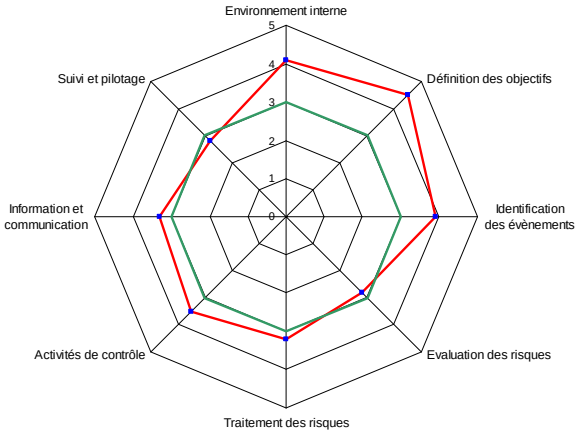
- la volonté managériale du service.

Un service obtient d'ores et déjà de très bonnes notes pour la majeure partie des dimensions du COSO. Un autre service est également déjà très avancé dans la formalisation de ses procédures. Deux services démontrent une réelle volonté de mettre en place une approche allant dans le sens d'une gestion intégrée des risques. Ils doivent poursuivre la voie entamée et concentrer leurs efforts sur la formalisation et la prise en compte de l'ensemble des risques. Un service s'est concentré essentiellement sur la gestion de ses risques métiers et doit entreprendre une approche plus globale.

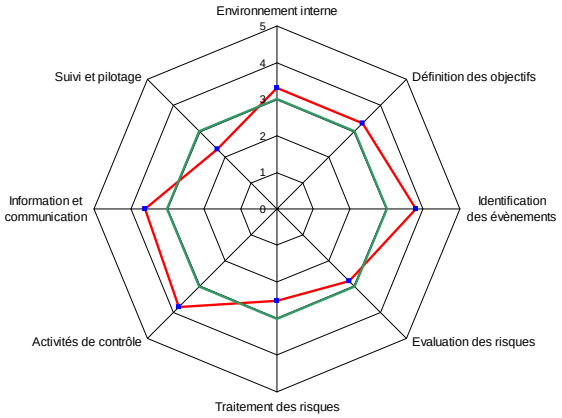
Représentation graphique de la maturité du processus de gestion des risques dans le service 1



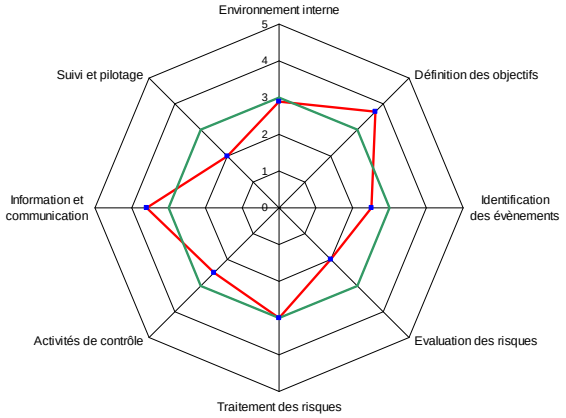
Représentation graphique de la maturité du processus de gestion des risques dans le service 2



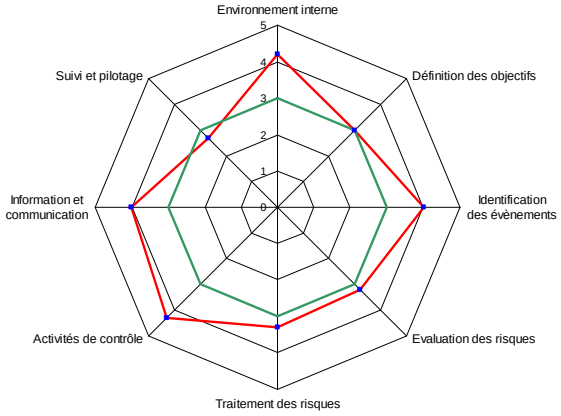
Représentation graphique de la maturité du processus de gestion des risques dans le service 3



Représentation graphique de la maturité du processus de gestion des risques dans le service 4



Représentation graphique de la maturité du processus de gestion des risques dans le service 5



CONCLUSIONS GÉNÉRALES

RAPPEL DES OBJECTIFS DE L'AUDIT

La vérification de l'évaluation de la gestion des risques est une des missions de la Cour selon la Loi sur la Cour des comptes (art. 24b).

Les objectifs du présent audit sont les suivants :

- Objectif 1 : faire un état des lieux des éléments de gestion intégrée des risques déjà existants au sein de cinq entités de l'administration cantonale vaudoise.
- Objectif 2 : apporter une valeur ajoutée relative à la conformité aux bonnes pratiques en matière de gestion intégrée des risques, et par là, améliorer la performance et le dynamisme de la gestion publique.

Les objectifs ont été atteints en répondant aux questions d'audit telles qu'elles sont exprimées dans les questionnaires qualitatifs et quantitatifs, regroupées autour des huit composantes du cube COSO. Ces questions d'audit relèvent de la méthodologie de la Cour des Comptes[40]. Les résultats de l'analyse sont présentés au chapitre précédent.

CONSTATATIONS ET RECOMMANDATIONS

Les entretiens avec la direction des entités auditées, ainsi que la consultation des documents mis à la disposition de la Cour ont permis à l'équipe d'audit de mettre en évidence les constatations et recommandations suivantes.

CONSTATATION N° 1

Malgré l'absence d'un référentiel de gestion des risques, les entités prennent en compte les risques dans leurs pratiques quotidiennes. L'approche est pragmatique et principalement orientée métiers.

Toutes les personnes auditées dans les différents services présentent une sensibilité marquée par rapport à la notion de risque. A travers l'analyse du questionnaire qualitatif, il ressort que, malgré l'absence d'un référentiel de gestion des risques à l'échelle de l'Etat, les entités prennent en compte les risques dans leurs pratiques quotidiennes.

Les services audités ont en particulier une maîtrise avérée de leurs risques métiers, c'est-à-dire liés directement aux prestations fournies par les services. Ainsi, les risques identifiés sont-ils essentiellement de type opérationnel.

Les services audités ne disposent cependant pas d'une approche intégrée des risques. La prise en compte des risques est, en général, d'abord pragmatique. Même si certaines procédures

[40] Manuel de vérification de l'évaluation de la gestion des risques, Méthodologie d'audit de la Cour des comptes du Canton de Vaud, volume 3, septembre 2009.

sont formalisées, il n'existe pas d'approche systématique en place, telle que celle proposée par le référentiel COSO par exemple (ou d'autres).

Notamment, il n'existe pas de lien formel entre la définition des objectifs et l'identification des risques. Ceux-ci ne sont pas formellement et systématiquement évalués. La réflexion sur le traitement à apporter aux risques, ainsi que les activités de contrôle, ne font pas partie d'un plan d'actions établi sur base de l'évaluation des risques.

De manière générale, les entités auditées ne définissent pas d'objectifs stratégiques à moyen terme, se concentrant principalement sur les objectifs opérationnels ou financiers. Ceux-ci ne sont pas mis en adéquation avec l'appétence au risque de l'Etat.

En outre, les entités ne disposent pas des documents suivants :

- une politique de gestion des risques
- un inventaire des risques
- une cartographie des risques (avec évaluation de l'impact et de l'occurrence).

Dans trois cas sur cinq, une approche intégrée des risques (avec inventaire et cartographie des risques financiers) est mise en place à travers un système de contrôle interne, axé uniquement sur les aspects financiers (directive 22).

Cela n'est pas suffisant puisque le volet stratégique, qui constitue une différence majeure entre le système de contrôle interne (basé sur le modèle COSO I) et la gestion intégrée des risques (basée sur le modèle COSO II), est absent.

RECOMMANDATION N°1

Dans la perspective d'appréhender et de traiter les risques auxquels l'Etat est confronté dans le développement de ses politiques publiques, les services de l'administration vaudoise devraient disposer des éléments suivants :

- un processus de fixation des objectifs à court et moyen terme (SMART)
- un inventaire des risques en lien avec les objectifs
- une évaluation des risques sur base de l'impact et de l'occurrence, de préférence schématisée dans une cartographie des risques
- des plans d'action, qui comprennent la décision de traitement à apporter au risque, avec les activités de contrôle y relatives et le propriétaire du risque
- un système d'information et de communication sur la gestion des risques, adapté et efficace
- une procédure de suivi et de pilotage du système de gestion des risques.

La DSI utilise une solution logicielle pour élaborer les schémas directeurs métier qui comporte également un module Gestion des risques. Les synergies qui pourraient exister entre ces logiciels devraient être examinées.

CONSTATATION N°2

Si la Cour a pu tirer des constats communs pour l'ensemble des services audités (voir constatation n° 1), le degré de maturité des composantes du COSO varie d'un service à l'autre et repose principalement sur la volonté managériale.

L'absence de lignes directrices ou de modèle proposé en matière de gestion intégrée des risques ne permet pas l'éclosion d'une culture du risque partagée au sein de l'Etat. Or, une vision globale est nécessaire pour donner l'impulsion à la mise en place d'une véritable gestion intégrée des risques au niveau stratégique, au-delà de l'approche opérationnelle.

RECOMMANDATION N°2

Selon certains chefs de service, l'impulsion pour passer à une réelle gestion intégrée des risques en tant qu'outil de pilotage stratégique doit venir du Conseil d'Etat.

La Cour recommande la mise en œuvre d'une gestion intégrée des risques au sein de l'administration cantonale vaudoise. Celle-ci doit inclure l'ensemble des risques qui peuvent influer sur la réalisation des objectifs de l'Etat, notamment ceux figurant dans le programme de législature.

Une approche de gestion des risques commune pour l'État de Vaud doit être définie au sein d'une politique de gestion des risques.

L'approche COSO II ou celle préconisée par des modèles similaires peut apporter une réelle valeur ajoutée dans le cadre de la mise en place de projets transversaux, notamment décrits dans le programme de législature 2012-2017 du Conseil d'Etat.

CONCLUSION

Même si certaines composantes, prises individuellement, sont bien développées au sein des entités auditées, la Cour ne peut pas conclure à l'existence d'un système de gestion intégrée des risques selon COSO II.

En effet, d'une façon générale, le processus de fixation des objectifs des services est peu formalisé. La relation entre objectifs et risques n'est pas établie, ce qui implique que l'ensemble des risques n'est pas couvert. Il n'existe pas d'évaluation des risques en termes d'impact et de probabilité d'occurrence. Une information et une communication spécifiques, ainsi que le suivi et le pilotage de la gestion des risques ne sont pas organisés.

La Cour peut toutefois souligner la bonne maîtrise des risques constatée dans les services audités et les inciter à la formaliser dans un système intégré de gestion des risques, qui inclurait notamment la dimension stratégique. De manière générale, les membres de la direction interviewés ont par ailleurs conscience de la plus-value apportée par un processus plus systématique et mieux formalisé en matière de gestion des risques, pour autant qu'il soit flexible et orienté sur les besoins du service. En particulier ceux qui ont déjà mis en place un système de contrôle interne certifié ont déjà une expérience de la méthodologie à appliquer.

Toutefois, un vrai système de gestion intégrée des risques n'a de sens que s'il est mis en place pour l'ensemble de l'administration vaudoise. En effet, un tel outil demande avant tout l'engagement total de la plus haute direction.

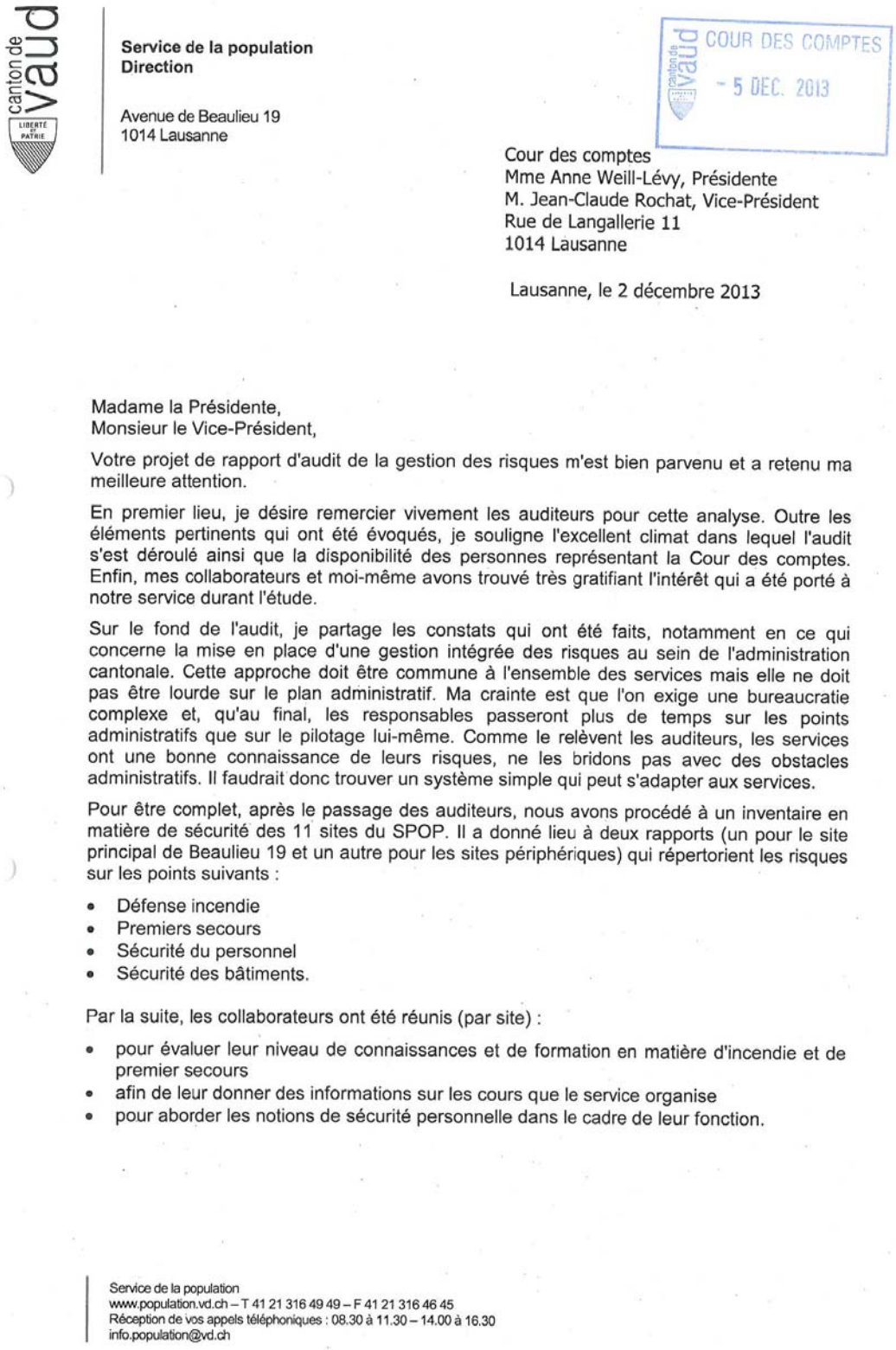
La Cour a pris connaissance de démarches importantes et transversales au sein de l'Etat qui vont dans le sens d'une gestion intégrée des risques : la mise en place d'un système de contrôle interne axé sur les risques liés aux états financiers, l'analyse des risques de sécurité informatique, la gestion intégrée des risques naturels[41].

La Cour estime que l'Etat pourrait profiter de l'énorme travail et de l'expérience acquise au travers de ces projets d'envergure pour créer des synergies et évoluer vers une gestion globale et intégrée des risques au sein de l'Etat, lui permettant d'avoir une vision générale de ses risques majeurs et de disposer ainsi d'un véritable outil de pilotage stratégique, à l'instar de ce qui existe à la Confédération ou dans de nombreuses autres administrations publiques.

[41] Voir chapitre 1, Les premiers jalons vers une gestion intégrée des risques dans l'administration vaudoise

OBSERVATIONS DES ENTITÉS AUDITÉES

Le projet de rapport a été soumis le 19 novembre aux entités auditées, afin qu'elles puissent formuler leurs observations, qui sont reproduites ci-dessous. Etant donné la portée générale des recommandations, le présent audit a également été envoyé au Chef du Département des Finances et des Relations Extérieures, dont la réponse figure en page 45.



canton de vaud
LIBERTÉ ET PATRIE

Service de la population
Direction

Avenue de Beaulieu 19
1014 Lausanne

COUR DES COMPTES
- 5 DEC. 2013

Cour des comptes
Mme Anne Weill-Lévy, Présidente
M. Jean-Claude Rochat, Vice-Président
Rue de Langallerie 11
1014 Lausanne

Lausanne, le 2 décembre 2013

Madame la Présidente,
Monsieur le Vice-Président,

Votre projet de rapport d'audit de la gestion des risques m'est bien parvenu et a retenu ma meilleure attention.

En premier lieu, je désire remercier vivement les auditeurs pour cette analyse. Outre les éléments pertinents qui ont été évoqués, je souligne l'excellent climat dans lequel l'audit s'est déroulé ainsi que la disponibilité des personnes représentant la Cour des comptes. Enfin, mes collaborateurs et moi-même avons trouvé très gratifiant l'intérêt qui a été porté à notre service durant l'étude.

Sur le fond de l'audit, je partage les constats qui ont été faits, notamment en ce qui concerne la mise en place d'une gestion intégrée des risques au sein de l'administration cantonale. Cette approche doit être commune à l'ensemble des services mais elle ne doit pas être lourde sur le plan administratif. Ma crainte est que l'on exige une bureaucratie complexe et, qu'au final, les responsables passeront plus de temps sur les points administratifs que sur le pilotage lui-même. Comme le relèvent les auditeurs, les services ont une bonne connaissance de leurs risques, ne les bridons pas avec des obstacles administratifs. Il faudrait donc trouver un système simple qui peut s'adapter aux services.

Pour être complet, après le passage des auditeurs, nous avons procédé à un inventaire en matière de sécurité des 11 sites du SPOP. Il a donné lieu à deux rapports (un pour le site principal de Beaulieu 19 et un autre pour les sites périphériques) qui répertorient les risques sur les points suivants :

- Défense incendie
- Premiers secours
- Sécurité du personnel
- Sécurité des bâtiments.

Par la suite, les collaborateurs ont été réunis (par site) :

- pour évaluer leur niveau de connaissances et de formation en matière d'incendie et de premier secours
- afin de leur donner des informations sur les cours que le service organise
- pour aborder les notions de sécurité personnelle dans le cadre de leur fonction.

Service de la population
www.population.vd.ch – T 41 21 316 49 49 – F 41 21 316 46 45
Réception de vos appels téléphoniques : 08.30 à 11.30 – 14.00 à 16.30
info.population@vd.ch

canton de vaud
Service de la population
Direction
Avenue de Beaulieu 19
1014 Lausanne

Un monitoring pour le suivi est en cours d'élaboration.

Enfin, dès le 1er juillet, le SPOP a une personne déléguée à 100% à la communication. Elle aura notamment pour tâche de faire une communication tant verticale qu'horizontale afin de véhiculer les valeurs de l'organisation, les objectifs et la gestion des risques.

En vous remerciant de l'attention que vous accorderez aux remarques ci-dessus, je vous prie d'agréer, Madame la Présidente, Monsieur le Vice-Président, mes salutations très distinguées.

Steve Maucci
Chef de service

Service de la population
www.population.vd.ch – T 41 21 316 49 49 – F 41 21 316 46 45
Réception de vos appels téléphoniques : 08.30 à 11.30 – 14.00 à 16.30
info.population@vd.ch

canton de vaud

Service des automobiles et de la navigation

Direction

Av. du Grey 110
1014 Lausanne

COUR DES COMPTES
10 DEC. 2013

Cour des comptes du canton de Vaud
Rue de Langallerie 11
1014 Lausanne

Réf. : SAN/PCY/efe

Lausanne, le 9 décembre 2013

Projet de rapport d'audit de la gestion des risques – *Analyse comparative dans cinq entités de l'administration cantonale vaudoise*

Madame, Monsieur,

Le projet de rapport mentionné en titre m'est bien parvenu et a retenu toute mon attention. Je tiens aussi à vous remercier de m'avoir donné la possibilité de m'exprimer concernant cet objet.

A cet égard, et après examen du projet de rapport, je vous informe que le Service des automobiles et de la navigation n'a pas d'observations particulières à formuler.

Toutefois, je relève qu'en page 14, le Contrôle cantonal des finances est abrégé CFF et qu'en page 15, il y a une faute à la fin du deuxième paragraphe de La Politique générale de sécurité des systèmes d'information [...]. Il est mentionné *d'acceptation des ces risques*.

En outre, je tiens à suggérer qu'il serait intéressant, pour les services concernés et ce avec leur accord, d'obtenir une version non anonymisée de ce rapport et ce afin de pouvoir comparer et améliorer les points audités.

En vous remerciant de l'attention portée à la présente, je vous présente, Madame, Monsieur, mes meilleures salutations.

Pascal Chatagny
Chef de Service

Service des automobiles et de la navigation - Département de la sécurité et de l'environnement
www.vd.ch/san – T + 41 21 316 88 04 – F + 41 21 316 88 08 – info.auto@vd.ch

canton de vaud
LIBERTÉ ET PATRIE

Le chef du Service de protection de la jeunesse

Av. Longemalle 1
1020 Renens

Cour des comptes
A l'att. de Mme la Présidente Anne Weill-Lévy et M. le Vice-Président Jean-Claude Rochat
Rue de Langallerie 11
1014 Lausanne

N/Réf. : CBO/eca – 691/13
(à rappeler dans toute correspondance)

021 316 53 46

Renens, le 9 décembre 2013

Observations générales relatives au rapport d'audit de la gestion des risques au sein du Service de protection de la jeunesse

Madame la Présidente,
Monsieur le Vice-Président,

Nous nous référons à votre courrier du 19 novembre dernier pour lequel nous vous remercions.

Tout d'abord, comme vous le mentionnez, aucune base légale actuelle n'impose aux Services de l'administration cantonale vaudoise la mise en place d'une évaluation formelle des risques.

Ensuite, la nature des missions dans différents services ne permet pas une même approche de la gestion des risques ; vous mentionnez d'ailleurs clairement cet aspect dans votre rapport. Au niveau du SPJ, l'approche de la Cour des comptes s'est focalisée sur une des quatre missions, certes la plus exposée, qui concerne la protection des mineurs. Il est utile de préciser ici les trois autres missions que sont la prévention, le soutien aux activités de la jeunesse, ainsi que l'autorisation et la surveillance des lieux d'accueils, sans oublier le domaine de l'adoption.

Le SPJ a construit depuis plusieurs années un référentiel, le SDO, système de direction et d'organisation, qui permet à chaque collaborateur de se référer aux normes et directives qui balisent le quotidien de la mise en œuvre de nos quatre missions.

Département de la formation, de la jeunesse et de la culture
Service de protection de la jeunesse
www.vd.ch/spj – T 41 21 316 53 46 – F 41 21 316 53 31

P:\SPJ\Chef de service\COURRIERS-DIVERS\Cour des comptes 9.12.13.doc

Après votre audit, nous trouvons intéressant de pouvoir prioriser certains risques en lien avec la « dimension relationnelle », emprunte d'humanité et d'émotionnel, ce qui est d'autant plus difficile, afin de formaliser leur approche et leur gestion. Nous ne pouvons objectivement que passer par une priorisation de ceux-ci, tant les moyens à mettre en place pour les maîtriser totalement, seraient trop importants. Mais, bien sûr, tel n'est pas le but de votre démarche, nous l'avons bien compris.

En ce qui concerne l'élaboration d'une cartographie des risques des services, le pas à franchir ne nous semble pas grand, pouvant nous référer aux nombreuses directives et procédures existantes au sein du Service. Elles sont mises à disposition et connues par l'ensemble des collaborateurs et elles n'empêchent pas aujourd'hui un pilotage contrôlé du Service, certes améliorable.

Vous remerciant pour vos constatations et recommandations qui ne permettront que d'améliorer la qualité de nos prestations, nous vous adressons, Madame la Présidente, Monsieur le Vice-Président, nos salutations distinguées.

Le Chef de service

Christophe Bornand

Gestion des risques
Pierre Schobinger A : Sandrine Neven 12.12.2013 17:00
Cc : Delphine Rouvé, Valérie Midili

Historique : Ce message a été transféré.

Madame,

Je me réfère à l'échange téléphonique que vous avez eu avec Mme Rouvé pour vous confirmer que nous n'avons pas de remarque ou d'observation à formuler.

En vous remerciant de nous avoir consulté, je vous de croire, Madame, à l'assurance de ma considération distinguée.

Pierre Schobinger
Secrétaire général de l'ordre judiciaire
Palais de justice de l'Hermitage
Route du Signal 8, CH-1014 Lausanne
Tél: +41 21 316 15 07 - Fax: +41 21 316 15 93
pierre.schobinger@vd.ch - http://www.vd.ch/ojv

Tr : Projet de rapport sur la gestion des risques
Jean-Claude Rochat A : Sandrine Neven, Eliane Rey 12.12.2013 18:43

----- Transféré par Jean-Claude Rochat/CdC/admin-VD le 12.12.2013 18:43 -----

De : Sylvie Bula/SPEN/admin-VD
A : Jean-Claude Rochat/CdC/admin-VD@admin-VD,
Date : 12.12.2013 18:41
Objet : Projet de rapport sur la gestion des risques

Monsieur le Vice-Président,

Je vous remercie pour l'envoi du rapport sur la gestion des risques, ainsi que de l'analyse spécifique pour le SPEN. Je vous prie de bien vouloir excuser mon absence de réponse dans les délais.

Je me permets de saluer l'important travail réalisé et l'intérêt des pistes d'amélioration que vous dégagez, tant dans votre rapport que dans l'analyse spécifique communiquée ultérieurement. Je n'ai pas de remarques particulières à formuler quant au contenu du rapport avant sa prochaine publication.

Je me tiens bien évidemment à votre disposition en cas de besoin et vous prie d'agréer, Monsieur le Vice-Président, mes salutations distinguées.

Sylvie Bula - Cheffe de service

Etat de Vaud, Département de l'intérieur
Service Pénitentiaire
Venoge Parc (Bâtiment A)
Ch. de l'Islettaz, CH-1305 Penthalaz
T : +41 21 316 48 01 F : +41 21 316 48 44
sylvie.bula@vd.ch www.vd.ch/spen

RÉPONSE DU CHEF DU DÉPARTEMENT DES FINANCES ET DES RELATIONS EXTÉRIEURES

De : Pascal Broulis/SG-DFIN/admin-VD
A : Jean-Claude Rochat/CdC/admin-VD@admin-VD,
Cc : Eric Birchmeier/SAGEFI/admin-VD@admin-VD
Date : 15.12.2013 15:01
Objet : RE: AUDIT SUR LA GESTION DES RISQUES DE 5 ENTITÉS

Monsieur le Magistrat responsable du dossier susmentionné,

Comme vous le mentionnez, l'Etat de Vaud s'attelle pour l'heure à la mise en oeuvre du SCI au sein de ses entités.
A moyen terme rien n'empêche l'examen des risques intégrés au regard des directives COSO II.

Avec mes respectueuses salutations.

Pascal Broulis
Conseiller d'Etat

ANNEXES

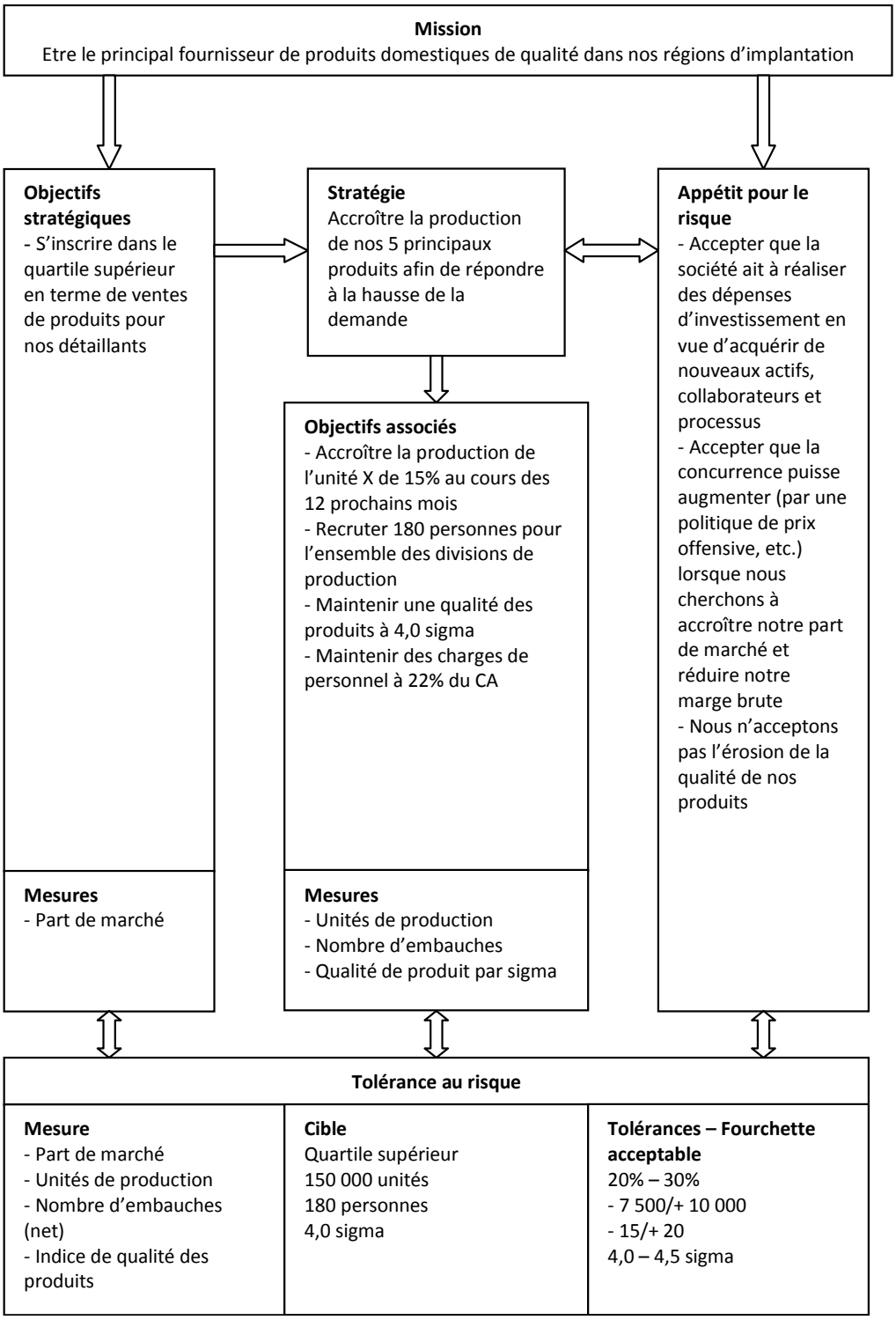
ANNEXE I : ELÉMENTS CLÉS DU DISPOSITIF DE MANAGEMENT DES RISQUES

Ce schéma est tiré de :

« Le management des risques de l'entreprise, Cadre de référence – Techniques d'application – COSO II Report », IFACI, Insitut de l'Audit Interne, PriceWaterHouseCoopers, Landwell & associés, Editions d'Organisation, 2005, p. 159.

Environnement interne Culture des risques – Appétence pour le risque – Conseil d'administration – Intégrité et valeurs éthiques – Engagement de compétence – Structure organisationnelle – Attribution des pouvoirs et responsabilités – Normes en matière de ressources humaines
Fixation des objectifs Objectifs stratégiques – Objectifs associés – Objectifs sélectionnés – Appétence pour le risque – Tolérance au risque
Identification des événements Evénements – Facteurs d'influence – Technique d'identification des événements – Lien entre les événements – Catégories d'événements – Distinction entre risques et opportunités
Evaluation des risques Risque inhérent et résiduel – Définition de la probabilité et de l'impact – Sources des données – Techniques d'évaluation – Relations entre les événements
Traitement des risques Evaluation des traitements possibles – Traitements choisis – Vision d'ensemble des risques
Activité de contrôle Intégration du traitement du risque – Type d'activités de contrôle – Politiques et procédures – Contrôles sur les systèmes d'information – Eléments spécifiques à l'entité
Information et communication Information – Communication
Pilotage Opérations courantes de pilotage – Evaluations spécifiques – Défaillances du système de reporting

ANNEXE II : RELATION ENTRE MISSION, OBJECTIFS, APPÉTENCE POUR LE RISQUE ET TOLÉRANCE AU RISQUE



Ce schéma est tiré de : « Le management des risques de l'entreprise, Cadre de référence – Techniques d'application – COSO II Report », IFACI, Insitut de l'Audit Interne, PriceWaterHouseCoopers, Landwell & associés, Editions d'Organisation, 2005, p. 184.

ANNEXE III : QUESTIONNAIRE QUALITATIF

Phase d'exécution de l'audit **Grille d'entretien qualitatif**				
Etabli par : **Date / visa**		**Validé par :** **Date / visa**	Magistrat(e) resp. :	Magistrat(e) suppl. :

Notre audit a pour but de faire un état des lieux des éléments de gestion des risques déjà existants au sein des services de l'Etat de Vaud et d'apporter une valeur ajoutée en termes de bonnes pratiques, qui pourrait déboucher sur une amélioration de la gestion et de la performance.

Il s'agit de conduire une mission parallèle dans cinq entités de l'Etat ce qui devrait nous permettre de comparer les approches utilisées.

Le but de l'audit n'est pas de se pencher sur les risques auxquels sont confrontés les services, mais sur leur manière de les identifier, de les évaluer et de les traiter, tout en accordant une importance particulière à l'environnement interne : les dirigeants et employés des services sont-ils sensibles au risque et quelle est la politique d'information et de communication sur ce thème au sein des services ?

La mission de la Cour n'est en effet pas d'évaluer les risques des services, cette tâche leur étant réservée. Elle est en revanche de vérifier l'évaluation de la gestion des risques et donc, d'examiner les processus mis en place à cet effet.

Pour mener à bien sa mission, la Cour, accompagnée d'experts en gestion des risques, a choisi de privilégier une double approche qualitative-quantitative. Nous procéderons donc dans un premier temps à un entretien semi directif afin de cerner l'environnement interne du service, puis nous continuerons sur un questionnaire quantitatif qui nous permettra de mesurer les autres éléments constitutifs d'une gestion des risques intégrée.

I. Environnement interne

L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs de l'entité, et plus particulièrement la conception du management et son appétence pour le risque, l'intégrité et les valeurs éthiques, et l'environnement dans lequel l'organisation opère.

1. Comment décririez-vous la culture du risque au sein de votre service ?

   Quel type de communication ? A qui s'adresse-t-elle ?

   Les politiques et processus organisationnels sont-ils respectés ?

   Comment la direction participe-t-elle à développer cette culture ?

   Pensez-vous qu'une gestion formalisée des risques apporte de la valeur ajoutée ?

   Quel est le degré de vigilance au sein du service ?

   Votre service s'appuie-t-il sur des normes ? Vous comparez-vous à d'autres services ?

2. Comment définiriez-vous la marge de manœuvre et l'attitude de votre service par rapport aux risques ? (appétence et tolérance au risque)

   Quelle est votre marge de manœuvre lors de prise de décision ? Vous satisfait-elle ?

   Votre service est-il sensible à l'existence de risques pouvant nuire à l'atteinte de vos objectifs ?

   Avez-vous le sentiment que votre service n'a pas suffisamment conscience des risques qu'il encourt ?

   Considérez-vous que les risques sont inévitables et inhérents au fonctionnement de votre organisation (il faut « faire avec ») ?

   Considérez-vous que la prise de risques est un moteur pour votre service ?

3. Comment évalueriez-vous la surveillance des risques par la direction du service ?

   Diriez-vous que vous/elle peut le faire de manière indépendante ?

   Diriez-vous que vous/elle est au bénéfice des compétences nécessaires à cette tâche ?

   Diriez-vous que vous/elle a suffisamment de temps à consacrer à cette tâche ?

4. Comment définiriez-vous le degré d'intégrité et les valeurs éthiques au sein de votre service ?

   Existe-t-il un document interne informant de ces valeurs ? Qu'en est-il des sanctions encourues ?

   Le personnel est-il informé par un autre biais ?

   La direction s'assure-t-elle que ces valeurs sont partagées ?

5. Pourriez-vous nous décrire la structure organisationnelle de votre service ?

   Disposez-vous d'un organigramme organisationnel ?

   Comment évaluez-vous l'état actuel de votre service (ressources, compétences, etc.)

6. Comment régulez-vous les responsabilités de chacun et éventuelles délégations de pouvoirs ?

   Existe-t-il un règlement tenant compte des risques associés à ces éléments ? Est-il connu par l'ensemble des collaborateurs ?

   Existe-t-il des normes et processus réglant les différents types d'accès (IT, locaux, ...)

7. Comment évalueriez-vous votre service du point de vue de la politique des ressources humaines ?

   Les cahiers des charges sont-ils adaptés ?

   Des possibilités de développement sont-elles proposées aux collaborateurs ?

   L'information relative aux cahiers des charges est disponible et connue de tous ?

   Une attention particulière est-elle portée sur des comportements immoraux ou malhonnêtes ?

ANNEXE IV : QUESTIONNAIRE QUANTITATIF

Phase d'exécution de l'audit **Questionnaire quantitatif**				
Etabli par : **Date / visa**		**Validé par :** **Date / visa**	Magistrat(e) resp. :	Magistrat(e) suppl. :

Notre audit a pour but de faire un état des lieux des éléments de gestion des risques déjà existants au sein des services de l'Etat de Vaud et d'apporter une valeur ajoutée en termes de bonnes pratiques, qui pourrait déboucher sur une amélioration de la gestion et de la performance.

Il s'agit de conduire une mission parallèle dans trois services de l'Etat ce qui devrait nous permettre de comparer les approches utilisées.

Le but de l'audit n'est pas de se pencher sur les risques auxquels sont confrontés les services, mais sur leur manière de les identifier, de les évaluer et de les traiter, tout en accordant une importance particulière à l'environnement interne : les dirigeants et employés des services sont-ils sensibles au risque et quelle est la politique d'information et de communication sur ce thème au sein des services ?

La mission de la Cour n'est en effet pas d'évaluer les risques des services, cette tâche leur étant réservée. Elle est en revanche de vérifier l'évaluation de la gestion des risques et donc, d'examiner les processus mis en place à cet effet.

Pour mener à bien sa mission, la Cour, accompagnée d'experts en gestion des risques, a choisi de privilégier une double approche qualitative-quantitative. Nous procéderons donc dans un premier temps à un entretien semi-directif afin de cerner l'environnement interne du service, puis nous continuerons sur un questionnaire quantitatif qui nous permettra de mesurer les autres éléments constitutifs d'une gestion des risques intégrée.

L'appréciation des différents éléments peut s'échelonner de 1 à 5, ces niveaux correspondant aux descriptions suivantes :

1 – Peu fiable : l'élément considéré est inexistant dans l'organisation.

2 – Informel : l'élément considéré existe dans l'organisation, mais de manière informelle (pas de documents probants).

3 – Standardisé : l'élément considéré existe dans l'organisation et est formalisé de manière basique.

4 – Surveillé : l'élément considéré est développé et documenté dans l'organisation.

5 – Optimisé : l'élément considéré est intégré au sein d'un processus de gestion des risques optimisé.

Le niveau à partir duquel on peut considérer que l'organisation a mis en place un système de gestion des risques est le niveau 3 – Standardisé.

II. Définition des objectifs

Les objectifs doivent avoir été préalablement définis pour que le management puisse identifier les évènements potentiels susceptibles d'en affecter la réalisation. Le management des risques permet de s'assurer que la direction a mis en place un processus de fixation des objectifs et que ces objectifs sont en ligne avec la mission de l'entité ainsi qu'avec son appétence pour le risque.

Comment qualifieriez-vous le niveau d'existence des objectifs en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Définition des objectifs (stratégiques, opérationnels, qualité des informations financières, conformité aux lois et règlements applicables)	☐	☐	☐	☐	☐
2	Mise en place de processus relatif à la définition des objectifs	☐	☐	☐	☐	☐
3	Communication des objectifs	☐	☐	☐	☐	☐
4	Politique interne de gestion des risques	☐	☐	☐	☐	☐

III. Identification des évènements

Les évènements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une organisation doivent être identifiés en faisant la distinction entre risques et opportunités. Les opportunités sont prises en compte lors de l'élaboration de la stratégie ou au cours du processus de fixation des objectifs.

Comment qualifieriez-vous le degré d'identification des évènements en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Niveau de compétence des personnes en charge de cette identification	☐	☐	☐	☐	☐
2	Existence d'une méthode	☐	☐	☐	☐	☐
3	Prise en compte multifactorielle des causes et origines	☐	☐	☐	☐	☐
4	Existence d'un inventaire	☐	☐	☐	☐	☐
5	Prise en compte des menaces et des opportunités	☐	☐	☐	☐	☐

IV. Evaluation des risques

Les risques sont analysés, tant en fonction de leur probabilité d'occurrence que de leur impact, cette analyse servant de base pour déterminer la façon dont ils doivent être gérés. Les risques inhérents et les risques résiduels sont évalués.

Comment qualifieriez-vous le degré d'évaluation des risques en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Niveau de compétence des personnes en charge de cette évaluation	☐	☐	☐	☐	☐
2	Existence d'une méthode d'estimation du risque	☐	☐	☐	☐	☐
3	Cohérence entre la période d'évaluation et la réalisation des objectifs	☐	☐	☐	☐	☐
4	Vérification de la fiabilité des données	☐	☐	☐	☐	☐
5	Existence d'une documentation relative à l'évaluation des risques	☐	☐	☐	☐	☐
6	Régularité dans l'évaluation des risques inhérents	☐	☐	☐	☐	☐

V. Traitement des risques

Le management définit des solutions permettant de faire face aux risques - évitement, acceptation, réduction ou partage. Pour ce faire, le management élabore un ensemble de mesures permettant de mettre en adéquation le niveau des risques avec l'appétence pour le risque de l'organisation. S'il n'y a pas de processus de gestion intégrée des risques, l'évaluation des activités de contrôle s'applique quand même à ce qui existe dans l'organisation.

Comment qualifieriez-vous le degré de traitement des risques en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Niveau de compétence des personnes en charge du traitement des risques	☐	☐	☐	☐	☐
2	Adoption de solution pour les risques évalués	☐	☐	☐	☐	☐
3	Evaluation systématique de la réponse à apporter et de la fiabilité des données	☐	☐	☐	☐	☐
4	Existence d'une documentation relative aux réponses apportées	☐	☐	☐	☐	☐
5	Proposition et validation des réponses par les personnes compétentes	☐	☐	☐	☐	☐
6	Evaluation régulière des réponses aux risques et du risque résiduel	☐	☐	☐	☐	☐

VI. Activités de contrôle

Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques. Dans certains cas, l'activité de contrôle constitue elle-même le traitement du risque. S'il n'y a pas de processus de gestion intégrée des risques, l'évaluation des activités de contrôle s'applique quand même à ce qui existe dans l'organisation.

Comment qualifieriez-vous les activités de contrôle en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Existence d'activité pour répondre aux risques ou s'assurer de l'application de la réponse proposée	☐	☐	☐	☐	☐
2	Retranscription des différentes activités de contrôle (sci)	☐	☐	☐	☐	☐
3	Communication des différentes activités de contrôle	☐	☐	☐	☐	☐
4	Vérification possible des activités de contrôle apportées	☐	☐	☐	☐	☐

VII. Information et communication

Les informations utiles sont identifiées, collectées et communiquées sous un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'organisation de façon efficace. S'il n'y a pas de processus de gestion intégrée des risques, l'évaluation de l'information et de la communication s'applique quand même à ce qui existe dans l'organisation.

Comment qualifieriez-vous le degré d'information et de communication en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Existence d'un système d'information fiable assurant l'identification, la collecte et la communication des informations	☐	☐	☐	☐	☐
2	Vérification de la qualité des informations fournies	☐	☐	☐	☐	☐
3	Communication des résultats de l'évaluation des risques à tout le personnel	☐	☐	☐	☐	☐
4	Définition claires et communication quant à la responsabilité de chacun pour ce qui a trait aux réponses à l'évaluation des risques	☐	☐	☐	☐	☐
5	Existence d'un canal de communication visant à faire remonter l'information	☐	☐	☐	☐	☐
6	Communication à l'externe de la manière de gérer les risques	☐	☐	☐	☐	☐

VIII. Suivi et pilotage

Le processus de management des risques est piloté dans sa globalité et modifié en fonction des besoins. Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités.

Comment qualifieriez-vous le degré de suivi et de pilotage en terme de :

		Peu fiable	Informel	Standardisé	Surveillé	Optimisé
N°	Eléments à évaluer	N'existe pas 1	Existe mais n'est pas documenté 2	Existe de manière basique et documentée 3	Existe de manière développée et documentée 4	Existe de manière optimisée 5
1	Existence d'un dispositif de pilotage à disposition de la direction	☐	☐	☐	☐	☐
2	Evaluations spécifiques ponctuelles du processus de gestion des risques	☐	☐	☐	☐	☐
3	Suivi du risque résiduel	☐	☐	☐	☐	☐

ANNEXE V : MODÈLE DE MATURITÉ

I. ENVIRONNEMENT INTERNE

L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs de l'entité, et plus particulièrement la conception du management et son appétence pour le risque, l'intégrité et les valeurs éthiques, et l'environnement dans lequel l'organisation opère.

Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
	1	2	3	4	5
CULTURE DU RISQUE					
1 Les principes de gestion des risques de l'entité sont communiqués a) une politique interne écrite spécifique à la gestion des risques de l'entité existe b) les principes de gestion des risques de l'entité sont évoqués ou rappelés dans d'autres politiques internes c) le personnel est informé par d'autres biais (ex : formation) d) la direction est assurée que l'ensemble du personnel est informé	Il n'existe pas de politique interne écrite spécifique à la gestion des risques, les principes de gestion des risques de l'entité ne sont ni évoqués, ni rappelés dans d'autres politiques internes, le personnel n'est pas informé par d'autres biais	Il existe une politique interne de gestion des risques, mais elle est diffuse, transmise surtout de manière orale. La direction n'est pas assurée que l'ensemble du personnel est informé.	La politique interne de gestion des risques est formalisée dans divers documents internes, mais il n'existe pas de politique interne spécifique. La direction est assurée que l'ensemble du personnel est informé.	Il existe une politique interne de gestion des risques, principalement liée à l'opérationnel. La direction est assurée que l'ensemble du personnel est informé.	Il existe une politique interne de gestion des risques qui fait partie inhérente du management. La direction est assurée que l'ensemble du personnel est informé.
2 Adhésion aux politiques, processus organisationnels	Valeurs individuelles de personnes fortes, rejet des politiques, procédures et acteurs transverses	Valeurs collectives existent, mais pas d'adhésion aux politiques, procédures transverses	Différents groupes font des actions différentes (adésion par silo)	En général, une adhésion moyenne au travers de l'entreprise. Quelques déviations persistent	Valeurs collectives intégrées, adhésion forte aux politiques, procédures transverses
3 Attitude de la direction face à la gestion des risques (prise en compte à la fois de la direction de l'organisation en tant qu'entité, mais également de l'influence exercée par le pouvoir politique en charge de l'entité)	N'apporte pas de support, voir hostile	Support passif, manque d'indépendance ou de compétence technique	Fait de la promotion dans son silo et support le concept	Fait de la promotion et encourage l'action dans toute l'organisation	Est un acteur "champion" avec une forte compréhension du système
4 Croyance de l'organisation dans la valeur ajoutée d'une gestion des risques formalisée.	La gestion des risques est vue comme une perte de temps inutile pouvant avoir un effet négatif	La gestion des risques est vue comme une distraction mais sans effet négatif	Perçue comme ayant une valeur ajoutée limitée pour toute l'organisation	Pense que la gestion des risques peut aider et apporter de la valeur	Pense que la gestion des risques peuvent améliorer la performance de l'organisation
5 Vigilance par rapport aux risques	Aucune vigilance dans l'ensemble de l'entreprise	Seuls quelques employés ou quelques entités sont vigilants aux risques. Pas de language commun à l'échelle de l'organisation.	Un language commun (glossaire) de risques existe pour l'ensemble de l'organisation. Tous les employés sont vigilants par rapport aux risques	Tous les employés sont conscients des risques et de leurs impacts par rapport à leurs objectifs personnels ou locaux	Tous les employés sont conscients des risques et de leurs impacts par rapport aux objectifs globaux de l'organisation.
6 L'organisation fait-elle partie d'associations professionnelles et respecte-t-elle les normes édictées par ces associations ?	L'organisation ne fait pas partie d'associations professionnelles, ne respecte pas ses normes et n'utilise pas ses prestations.	L'organisation ne fait pas partie d'associations professionnelles mais applique en partie ses normes ou utilise occasionnellement ses prestations.	L'organisation est membre d'associations professionnelles, respecte ses normes et utilise occasionnellement ses prestations.	L'organisation est membre d'associations professionnelles et les normes sont intégrées à la gestion de l'organisation.	L'organisation est membre actif d'associations professionnelles et les normes professionnelles influencent les objectifs stratégiques de l'organisation.
APPETENCE AU RISQUE					
7 Appétence et tolérance au risque L'appétence au risque est le degré d'incertitude acceptable par la direction générale pour avoir une assurance raisonnable que soient atteints ses objectifs de création de valeur. La tolérance au risque désigne les niveaux acceptables de variation dans l'atteinte des objectifs (qu'est-ce qui est "raisonnable"). Le management des risques doit aider la direction à adopter des stratégies correspondant à l'appétence et à la tolérance au risque de l'organisation.	Soit une forte aversion au risque ou une prise de risque sans aucune conscience ou connaissance des risques	Compréhension intuitive du niveau de risque que l'organisation est prête à accepter	Prise de conscience par la direction de l'importance de prendre des risques appropriés à l'organisation, l'appétence au risque est formalisée de manière sommaire.	Conscience établie du besoin de mesurer l'appétit au risque (mesure de l'appétence au risque dans l'organisation, avec un questionnaire par exemple) et mise en place d'une approche globale	Suivi continu de l'appétit et de la tolérance au risque de l'organisation et quantification financière du risque résiduel
SURVEILLANCE					
8 La surveillance qu'exerce la direction de l'organisation est adéquate car elle est a) indépendante (par rapport au pouvoir exécutif, pas de conflits d'intérêt) compétente (connaissances techniques et expérience suffisantes) b) suffisante (en temps et en moyens, degré d'implication) c)	La surveillance n'est ni indépendante, ni compétente, ni suffisante	La surveillance est faible, car deux des trois critères ne sont pas respectés	La direction exerce une surveillance de base, néanmoins un des critères n'est pas respecté.	Les trois critères sont respectés	La surveillance est particulièrement adéquate puisqu'intégrée dans une politique de gestion des risques

INTEGRITE ET VALEURS ETHIQUES						
9	Les valeurs d'éthique de l'entité et les questions d'intégrité et de conflits d'intérêt sont mises en avant a) un document interne existe b) le personnel est informé par d'autres biais (ex : formation) c) la direction est assurée que l'ensemble du personnel est informé	Aucun document relatif aux valeurs éthiques ou aux questions d'intégrité et de conflits d'intérêt n'existe dans l'organisation	Il existe une culture éthique dans l'entreprise, liée aux personnes ou aux métiers, mais rien n'est formalisé. La direction n'est pas assurée que l'ensemble du personnel est informé	Un code éthique propre au groupe ou à la branche auquel appartient l'organisation existe, se limitant en général au simple respect des normes légales minimales. La direction n'est pas assurée que l'ensemble du personnel est informé.	Un code éthique propre au groupe ou à la branche auquel appartient l'organisation est développé (contient des normes éthiques et comportementales) et la direction est assurée que l'ensemble du personnel est informé (signature à l'engagement).	Un code éthique élaboré spécifiquement par l'organisation existe et la direction fait en sorte qu'il soit complètement intégré par l'ensemble du personnel (formation, signature à l'engagement). La direction s'investit dans son rôle d'exemple.
10	Des dispositions règlent le traitement des éventuels manquements au respect des règles d'éthique ou des principes de gestion des risques. La direction est assurée que l'ensemble du personnel en a connaissance	Non	Le personnel a conscience de ce qu'il encourt en cas de manquements au respect des règles d'éthique ou des principes de gestion des risques, mais ce n'est pas formalisé et la direction n'est pas assurée que l'ensemble du personnel en a connaissance.	Des dispositions règlant les éventuels manquements existent, mais la direction n'est pas assurée que le personnel en a connaissance	Des dispositions règlant les éventuels manquements existent et la direction est assurée que l'ensemble du personnel est informé (signature à l'engagement).	Des dispositions règlant les éventuels manquements existent, qui font partie de la véritable culture éthique mise en place dans l'organisation. La direction est assurée que l'ensemble du personnel est informé (signature à l'engagement) et tient à faire respecter les principes éthiques.
STRUCTURE ORGANISATIONNELLE						
11	La structure et l'organisation de l'entité sont a) clairement définies et documentées b) adaptées à sa taille et la complexité de ses tâches	L'organisation n'est ni structurée, ni organisée.	L'organisation est structurée et organisée mais la culture orale prévaut : chacun sait ce qu'il a à faire.	La structure et l'organisation de l'entité font l'objet d'une formalisation écrite, mais ne s'inscrit pas dans une recherche d'optimisation en fonction de sa taille et de la complexité de ses tâches.	La structure et l'organisation de l'entité font l'objet d'une formalisation écrite, réflexion sur optimisation au niveau opérationnel, en fonction de sa taille et de la complexité de ses tâches (revue régulièrement).	La structure et l'organisation de l'entité ont été pensées et documentées dans la statégie et la politique de risques de l'organisation.
DELEGATION DES POUVOIRS ET DES RESPONSABILITES						
12	La délégation des pouvoirs et responsabilités fait l'objet d'un règlement qui prend en compte la politique des risques de l'entité a) qui est connu de l'ensemble des collaborateurs b)	Il n'existe pas de délégation des pouvoirs et responsabilités claires dans l'organisation	Il y a une délégation des pouvoirs et responsabilités mais non formalisée dans un règlement. Elle ne prend pas formellement en compte la politique des risques de l'entité et n'est pas nécessairement connue de l'ensemble des collaborateurs.	La délégation des pouvoirs et responsabilités fait l'objet d'un règlement qui est connu de l'ensemble des collaborateurs.	La délégation des pouvoirs et responsabilités fait l'objet d'un règlement qui est connu de l'ensemble des collaborateurs. Ceux-ci sont conscients des risques associés à leurs responsabilités et des procédures sont mises en place pour contrôler les résultats.	La délégation des pouvoirs et responsabilités fait l'objet d'un règlement qui est connu de l'ensemble des collaborateurs et fait partie de la stratégie de l'organisation, notamment au niveau de l'optimisation de sa politique des risques.
13	Les processus et normes régissant l'attribution des droits d'accès aux systèmes et aux locaux sont définis et connus	Il n'existe pas de processus et normes régissant l'attribution des droits d'accès aux systèmes et aux locaux	Il existe des processus et normes régissant l'attribution des droits d'accès aux systèmes et aux locaux, mais ils ne sont pas documentés.	Il existe un document formalisé sur les droits d'accès aux systèmes et aux locaux.	Les processus et normes régissant l'attribution des droits d'accès aux systèmes et aux locaux font l'objet d'une formalisation claire et connue de tous, de manière à optimiser la gestion opérationnelle des activités.	Les processus et normes régissant l'attribution des droits d'accès aux systèmes et aux locaux sont optimisées en fonction de la politique des risques de l'organisation.

POLITIQUE DE RESSOURCES HUMAINES						
14	La concordance entre le cahier des charges et les compétences du collaborateur engagé pour le poste est assurée; des mesures relatives au suivi du développement des compétences des collaborateurs et de leur concordance avec le cahier des charges sont édictées et disponibles	Non.	La concordance et le suivi sont informels.	Il existe une procédure formelle d'évaluation et de suivi des compétences, et de leur concordance au cahier des charges, mais elle se réduit le plus souvent à un simple entretien.	Il existe une procédure formelle d'évaluation et de suivi des compétences, ainsi que leur concordance au cahier des charges. La manière dont l'évaluation et le suivi sont effectués et les points abordés sont également formalisés. Le modèle utilisé est le plus souvent un modèle de référence.	Il existe une procédure formelle d'évaluation et de suivi des compétences, ainsi que leur concordance au cahier des charges. La manière dont l'évaluation et le suivi sont effectués et les points abordés sont également formalisés. Le modèle utilisé a été développé spécifiquement pour l'organisation et le résultat de ces évaluations sert la stratégie et la politique de risques de l'organisation.
15	Les éléments susceptibles de générer un comportement immoral ou malhonnête des collaborateurs sont identifiés. Des mesures sont mises en place pour éviter/déceler/traiter les risques de fraude ou de vol interne.	L'organisation ne conçoit pas que les collaborateurs puissent se comporter de manière immorale ou malhonnête.	La culture éthique de l'organisation, la qualité des collaborateurs et le contrôle permanent sont des éléments qui peuvent donner une assurance raisonnable que le risque de comportement immoral ou malhonnête des collaborateurs est faible. Pas de formalisation.	Des mesures minimales sont mises en place pour éviter/déceler/traiter le risque de comportement immoral ou malhonnête des collaborateurs. Celles-ci sont connues de l'ensemble du personnel.	La direction a identifié clairement dans un document spécifique les éléments susceptibles de générer un comportement immoral ou malhonnête des collaborateurs. Des mesures minimales sont mises en place pour éviter/déceler/traiter le risque de comportement immoral ou malhonnête des collaborateurs. Celles-ci sont connues de l'ensemble du personnel.	La direction a identifié clairement dans un document spécifique les éléments susceptibles de générer un comportement immoral ou malhonnête des collaborateurs et elle a mis en place des procédures de contrôle et de détection, en ligne avec la politique des risques de l'organisation.

II. DEFINITION DES OBJECTIFS

Les objectifs doivent avoir été préalablement définis pour que le management puisse identifier les évènements potentiels susceptibles d'en affecter la réalisation. Le management des risques permet de s'assurer que la direction a mis en place un processus de fixation des objectifs et que ces objectifs sont en ligne avec la mission de l'entité ainsi qu'avec son appétence pour le risque.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
1	Les objectifs de l'entité sont définis formellement et incluent : a) les objectifs stratégiques b) les objectifs opérationnels c) la qualité des informations financières d) la conformité aux lois et règlements applicables	Aucun document ne formalise les objectifs de l'entité.	Les objectifs de l'organisation sont formalisés de manière générale, le plus souvent par une loi ou un règlement externe. L'organisation se contente de respecter les lois et règlements (conformité et régularité).	Les objectifs de l'organisation sont formalisés spécifiquement à l'intérieur de l'organisation, mais dans les grandes lignes (déclaration de mission de l'entité)	Les objectifs de l'organisation sont clairement formalisés, et assure à la direction de disposer d'informations de qualité pour la prise de décision, le contrôle des activités et des performances de l'organisation (objectifs opérationnels).	Les objectifs de l'organisation sont clairement formalisés, y compris les objectifs opérationnels à court terme et les objectifs stratégiques à moyen et long terme. Ils tiennent compte de l'appétence et de la tolérance au risque de l'organisation
2	Il existe un processus de fixation des objectifs	Non	Des discussions informelles ont lieu par rapport aux objectifs de l'organisation	Il existe un processus minimum de fixation des objectifs	Les objectifs sont fixés selon un processus clair et développé, ils sont revus régulièrement afin de les adapter à la mission de base de l'organisation et à l'évoluation de son environnement	Les objectifs sont fixés selon un processus clair et développé, ils sont revus régulièrement afin de les adapter à la mission de base de l'organisation et à l'évoluation de son environnement. Ils tiennent compte de l'appétence et de la tolérance au risque de l'organisation.
3	Si des objectifs ont été définis, sont-ils communiqués à l'ensemble du personnel ?	Pas d'objectifs ou ils ne sont connus que par le top management	Les objectifs ne sont connus que par les cadres supérieurs	Les objectifs sont censés être connus de tous, mais la direction ne peut s'en assurer	Les objectifs sont censés connus de tous (la direction peut s'en assurer car un document est distribué ou affiché).	Tout le personnel connaît les objectifs et a reçu une explication à ce sujet.
4	Si une politique interne de gestion des risques existe, ses objectifs sont-ils clairement définis ?	Les objectifs ne sont pas définis et le personnel ne sait pas quelle est la valeur ajoutée de la politique de gestion des risques	Les objectifs ne sont pas définis, mais le personnel a une culture des risques et comprend la valeur ajoutée de la politique interne de gestion des risques	Les objectifs de la politique interne sont définis de manière générale en référence à des modèles existants.	Les objectifs de la politique interne de gestion des risques sont développés, ils incluent les objectifs opérationnels, relatifs à la performance de l'organisation	Les objectifs de la politique interne de la gestion des risques sont en lien avec les objectifs stratégiques de l'organisation et son appétence et sa tolérance au risque

III. IDENTIFICATION DES EVENEMENTS

Les évènements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une organisation doivent être identifiés en faisant la distinction entre risques et opportunités.
Les opportunités sont prises en compte lors de l'élaboration de la stratégie ou au cours du processus de fixation des objectifs.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
1	L'identification des évènements est effectuée par les personnes les plus compétentes pour l'effectuer (implication des responsables opérationnels à tous les niveaux et de la direction)	Pas d'identification préalable.	L'identification a été réalisée par la direction	L'identification est réalisée par la direction et les cadres supérieurs, et une remontée d'informations des responsables opérationnels est possible	L'identification a été réalisée par la direction sur base d'un processus de consultation des responsables opérationnels	L'identification a été réalisée avec l'implication de tout le personnel concerné. Des procédures sont mises en place pour identifier les évènements.
2	Une méthode reconnue d'identification est suivie	Non, les risques sont identifiés après leur réalisation.	L'identification repose sur l'expertise des collaborateurs à l'interne	L'identification repose sur l'expertise des collaborateurs en interne, sur une veille des risques arrivant aux organisations similaires ou sur un catalogue général des risques	Un catalogue de risques établi spécifiquement pour l'organisation existe pour renforcer l'identification des risques basée sur l'expertise et la veille . Ce catalogue est régulièrement mis à jour et documenté.	L'identification repose sur un ensemble de méthodes (catalogues de risques, brainstorming, entretiens, questionnaire, analyse interne, …), rétrospectives mais aussi prospectives
3	Tous les types de facteurs qui influencent les évènements sont considérés : a) économiques b) environnementaux c) politiques d) sociaux e) technologiques (évènements internes ou externes) f) infrastructures g) personnel h) processus	Aucun facteur n'a été considéré	Moins de la moitié des facteurs ont été considérés.	Au moins la moitié des facteurs ont été considérés	La majorité des facteurs ont été considérés	Tous les facteurs ont été considérés
4	L'inventaire est : a) documenté b) remis à jour régulièrement c) fait état des interdépendances entre les évènements	L'inventaire n'est pas documenté	L'inventaire est documenté	L'inventaire est documenté et remis à jour ponctuellement	L'inventaire est documenté et remis à jour ponctuellement. Il comporte un classement par catégories d'évènements (par causes ou conséquences) pour cerner les liens existant entre eux et obtenir un meilleur niveau d'information	L'inventaire est documenté et fait état des interdépendances entre les évènements. Il constitue un véritable outil de gestion stratégique, il est régulièrement remis à jour.
5	Les différentes faces du risque (menace et opportunité) sont prises en compte	Aucun processus de gestion des risques n'existe	La nuance entre menace et opportunité n'a jamais été faite par l'organisation qui s'est toujours concentré intuitivement sur les menaces	Tout le processus et le système de gestion des risques est conçu pour analyser volontairement uniquement les menaces, mais l'organisation prend conscience de ses opportunités.	Tout le processus et le système de gestion des risques est conçu pour analyser les menaces et les opportunités (risque de ne pas prendre de risques).	Tout le processus et le système de gestion des risques est conçu pour analyser les menaces et les opportunités. Cette logique est poussée jusqu'au choix des solutions afin de profiter des opportunités pour financer les conséquences des menaces.

IV. EVALUATION DES RISQUES

Les risques sont analysés, tant en fonction de leur probabilité d'occurrence que de leur impact, cette analyse servant de base pour déterminer la façon dont ils doivent être gérés. Les risques inhérents et les risques résiduels sont évalués.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
1	L'évaluation des risques identifiés est effectuée par les personnes les plus compétentes pour l'effectuer (implication des responsables opérationnels à tous les niveaux et de la direction)	Pas d'évaluation	L'évaluation est réalisée par la direction uniquement.	L'évaluation est réalisée par la direction et les cadres supérieurs. L'organisation est assurée que ceux-ci sont des spécialistes possédant toutes les compétences requises en matière d'évaluation des risques et qu'ils ont bien compris le système de notation.	L'évaluation est réalisée sur base d'entretiens et d'ateliers avec le personnel concerné. L'organisation est assurée que ceux-ci sont des spécialistes possédant toutes les compétences requises en matière d'évaluation des risques et qu'ils ont bien compris le système de notation.	L'évaluation est réalisée sur base de méthodes quantitatives et qualitatives développées, par des spécialistes en risque et avec l'implication du personnel. Celui-ci a intégré le système de notation.
2	Quelle méthode d'estimation du risque est utilisée ?	Pas d'estimation	Seul un indice de risque est donné. Pas de distinction entre probabilité et gravité.	La probabilité et l'impact des risques sont donnés, seule une estimation en valeur brute est donnée	La probabilité et l'impact des risques sont donnés, une estimation risque par risque est donnée en valeur brute et en valeur nette	La probabilité et l'impact des risques sont donnés, une agrégation des risques est réalisée au niveau d'indicateur de performance de l'organisation, la corrélation entre évènements a été prise en compte
3	La période considérée pour l'évaluation est cohérente avec celle fixée pour la réalisation des objectifs	Pas d'estimation	L'estimation ne tient pas formellement compte de la période considérée	Une période est donnée pour l'évaluation des risques mais pas de recherche de cohérence avec les objectifs	La période considérée pour l'évaluation a été mise en ligne avec les objectifs	La période considérée pour l'évaluation est cohérente avec celle fixée pour la réalisation des obectifs et la recherche de cohérence sert à maximiser le processus d'évaluation
4	La fiabilité des données est vérifiée	Pas d'estimation	Le risque est estimé intuitivement	L'estimation est basée sur des données existantes	Les données ont été formellement testées	La base de données a été construite et les données vérifiées
5	Le résultat de l'évaluation des risques est documenté	Aucune documentation	Liste des risques avec indication de l'indice de risque	Liste des risques avec probabilité et impact	Cartographie des risques avec mise en évidence des priorités de l'organisation en matière de risques (lien avec l'appétence au risque de l'organisation)	Cartographie des risques détaillée avec mise en évidence des priorités de l'organisation en matière de risques (lien avec l'appétence au risque de l'organisation) et agrégation du risque tenant compte des interactions entre les risques majeurs
6	Les risques inhérents sont réévalués régulièrement	Jamais	De manière informelle et limitée, suite à un dysfonctionnement ou une modification dans l'organisation	De manière globale, lorsque les objectifs ou la structure de l'organisation sont modifiés	Les risques sont réestimés tous les 2 ou 3 ans	Les risques sont réestimés tous les ans dans le cadre de la procédure d'évaluation de la gestion des risques

V. TRAITEMENT DES RISQUES

Le management définit des solutions permettant de faire face aux risques - évitement, acceptation, réduction ou partage. Pour ce faire, le management élabore un ensemble de mesures permettant de mettre en adéquation le niveau des risques avec l'appétence pour le risque de l'organisation.
S'il n'y a pas de processus de gestion intégrée des risques, l'évaluation des activités de contrôle s'applique quand même à ce qui existe dans l'organisation.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
1	L'évaluation des solutions à apporter aux risques identifiés est effectuée par les personnes les plus compétentes pour l'effectuer (implication des responsables opérationnels à tous les niveaux et de la direction)	Pas d'évaluation	L'évaluation a été réalisée par la direction	L'évaluation a été réalisée par la direction et des cadres supérieurs. L'organisation est assurée que ceux-ci sont des spécialistes possédant toutes les compétences requises en matière d'évaluation des risques.	L'évaluation a été réalisée sur base d'entretiens et d'ateliers avec le personnel concerné. L'organisation est assurée que ceux-ci sont des spécialistes possédant toutes les compétences requises en matière d'évaluation des solutions.	L'évaluation a été réalisée sur base de recherches développées par des spécialistes en risque et avec l'implication du personnel
2	Une solution a été adoptée pour chacun des risques évalués	L'évaluation des risques ne débouche pas sur une réflexion sur le traitement des risques	Une réflexion non formalisée débouche sur des actions de traitement des risques	Selon son appétence au risque, l'organisation a choisi pour chacun des risques ou pour les risques majeurs évalués sa stratégie (évitement, réduction, partage, acceptation)	L'organisation a choisi pour chacun des risques évalués sa stratégie (évitement, réduction, partage, acceptation). Une fois les actions de traitement en place, l'organisation examine chaque risque, chaque traitement ainsi que l'adéquation du risque résiduel (impact et probabilité) au seuil de tolérance.	L'organisation a choisi pour chacun des risques évalués sa stratégie (évitement, réduction, partage, acceptation). Une fois les actions de traitement en place, l'organisation examine chaque risque, chaque traitement ainsi que l'adéquation du risque résiduel au seuil de tolérance, en tenant compte des effets cumulés des actions de traitement et également de l'impact positif des opportunités.
3	Une évaluation précise de la meilleure réponse est effectuée systématiquement et la fiabilité des données est vérifiée.	Pas d'évaluation de traitement des risques	Certaines actions de traitement des risques sont décidées et mises en œuvre sans avoir recours à une analyse (en réactivité à la réalisation de risques). Poursuite des habitudes de gestion.	Généralement, seule une solution de traitement est proposée pour un risque donné. La solution repose sur des données fiables mais pas de recherche d'alternative.	L'organisation utilise l'ensemble des solutions de traitement de risques (réduction et financement). Plusieurs solutions sur base de données fiables sont proposées avant décision. Le traitement du risque s'effectue risque par risque et tient compte de l'appétence et de la tolérance au risque de l'organisation.	L'organisation a recours à une gestion de type portefeuille de risques (les gains de certains risques peuvent être utilisés pour financier les pertes de certaines menaces). Optimisation du coût du risque et du meilleur traitement global des risques sur base de données fiables (approche coûts-bénéfices). Les solutions sont mises en lien avec l'appétence et la tolérance au risque de l'organisation.
4	Les réponses aux risques (et opportunités) sont documentées.	Aucune documentation n'est disponible	Les actions de traitement sont formalisées dans certains documents.	La documentation des actions de traitement est formalisée dans un document spécifique (plan d'action) sous la responsabilité d'une personne.	Le plan d'action est accessible au plus grand nombre. Elle est utilisée pour mettre à jour la valeur du risque concerné après réalisation de l'action. Un responsable d'action est clairement identifié.	Un système d'information est mis en place transversalement au sein de l'organisation afin de stocker l'ensemble des données relatives aux actions de traitement des risques et pour gérer leur avancement
5	Les réponses aux risques choisies sont approuvées par les personnes autorisées (la décision est-elle tracée ?)	Non.	Oui, mais pas de trace formelle.	Oui (PV)	Oui, un processus existe.	Oui, un processus détaillé existe de manière à optimiser les réponses aux risques (responsables du risque désignés)

6	Les réponses aux risques et le risque résiduel sont réévaluées régulièrement	Jamais	De manière informelle et limitée, lors d'un dysfonctionnement ou une modification significative d'un élément de l'organisation.	Réflexion globale, suite à un dysfonctionnement ou lorsque les objectifs ou la structure de l'organisation est modifiée	Les plans d'actions sont réestimés tous les 2 ou 3 ans	Les plans d'actions sont réestimés tous les ans dans le cadre de la procédure d'évaluation de la gestion des risques

VI. ACTIVITES DE CONTRÔLE

Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques.
Dans certains cas, l'activité de contrôle constitue elle-même le traitement du risque.
S'il n'y a pas de processus de gestion intégrée des risques, l'évaluation des activités de contrôle s'applique quand même à ce qui existe dans l'organisation.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
1	Des activités de contrôle sont mises en place pour répondre aux risques directement ou pour s'assurer que les solutions prévues sont appliquées.	Pas d'activités de contrôle	Des activités de contrôle minimum sont mises en place, en général pour des obectifs de conformité (besoins "vitaux" de l'organisation)	Des activités de contrôle sont mises en place pour garantir les objectifs de conformité et de régularité.	Les activités de contrôle sont développées de manière à garantir la réalisation des objectifs opérationnels de l'organisation.	Les activités de contrôle sont mises en place de manière à optimiser la politique de gestion des risques de l'organisation.
2	Les activités de contrôle sont définies par écrit (système de contrôle interne)	Pas d'activités de contrôle	Les activités existent mais ne sont pas documentées (culture orale)	Les activités existent et sont documentées dans des divers documents	Les activités existent et sont documentées dans un seul document spécifique	Les activités de contrôle sont documentées dans la politique de risques et sont en adéquation avec les objectifs et la stratégie risques de l'organisation.
3	Les activités de contrôle définies sont connues de l'ensemble du personnel.	Pas d'activités de contrôle	Les activités de contrôle sont mises en place par la direction et connues uniquement des cadres supérieurs	Les activités de contrôle sont connues par les responsables concernés.	Les activités de contrôle sont connues par les responsables concernés et par la majorité du personnel.	Un système d'information est mis en place qui assure que la politique, les procédures de contrôle et leur lien avec la politique des risques sont connues de l'ensemble du personnel.
4	Les activités de contrôle sont vérifiables (évidence du contrôle)	Pas d'activités de contrôle	La vérifiabilité des activités de contrôle se basent sur la confiance dans les responsables concernés et dans le système d'information, mais pas de formalisation.	Les activités de contrôle ont été mises en place en s'assurant qu'elles puissent être vérifiables.	Les activités de contrôle ont été mises en place s'assurant qu'elles puissent être vérifiables et sont régulièrement contrôlées.	Un système de contrôle et d'information permanent est mis en place afin de s'assurer que les activités de contrôle ont les résultats escomptés.

VII. INFORMATION ET COMMUNICATION

Les informations utiles sont identifiées, collectées et communiquées sous un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'organisation de façon efficace.
S'il n'y a pas de processus de gestion intégrée des risques, l'évaluation de l'information et de la communication s'applique quand même à ce qui existe dans l'organisation.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
INFORMATION						
1	Il existe un système d'information fiable assurant que les informations nécessaires à la réalisation des objectifs soient identifiées, collectées et communiquées.	Les informations ne circulent pas	Système d'information informel (basé sur la tradition orale, au cas par cas).	Le système d'information repose sur certains processus formels existants dans l'organisation pour des objectifs de reporting et de conformité	Le système d'information repose sur des processus formels existants dans l'organisation pour des objectifs opérationnels, de reporting et de conformité	Le système d'information repose sur des processus garantissant que l'ensemble des informations nécessaires au management des risques soit disponibles (systèmes stratégiques et intégrés)
2	La qualité des informations est vérifiée : les informations doivent être adéquates (suffisantes et pertinentes), actuelles, exactes, accessibles et disponibles en temps utile	Les informations sont de mauvaise qualité (au moins 2 critères non respectés)	La qualité des informations n'est pas vérifiée	La qualité des informations de base liées à la conformité et à la régularité est vérifiée	La qualité des informations liées à la conformité, la régularité et l'opérationnel est vérifiée	La qualité des informations est optimisée par le système mis en place de manière à garantir la mise en place de la stratégie de l'organisation
COMMUNICATION						
3	Le résultat de l'évaluation des risques (objectifs, identification, évaluation et solutions) est communiqué à tout le personnel	Pas de communication.	Le résultat de l'évaluation reste au niveau du management avec éventuellement une communication partielle au personnel directement concerné. La communication interne n'est pas souhaitée.	La stratégie sur les risques est communiquée aux responsables opérationnels.	La stratégie face aux risques et le processus sont communiqués dans toute l'organisation.	Communication large dans l'entreprise, support du personnel et atttitude engagée de la direction (culture d'entreprise)
4	Les responsabilités de chaque employé envers les réponses à l'évaluation des risques sont clairement définies et communiquées	Les rôles et les responsabilités ne sont définis dans aucun document	Les rôles et responsabilités en matière de gestion des risques sont sous-entendus dans les rôles et responsabilités généraux	Quelques rôles sont définis en matière de gestion des risques. Cette description est faite sans mettre en avant un partage clair des responsabilités associées à la gestion des risques	Les rôles et responsabilités en matière de gestion des risques sont définis dans l'organisation et connus de tous	Les rôles et responsabilités en matière de gestion des risques sont définis dans politique de gestion des risques et expliquées à tout le personnel pour s'assurer que chacun se sente impliqué, et conscient des interactions entre leurs activités et celles des autres.
5	Un canal de communication permet aux employés d'informer leur hiérarchie sur les possibilités d'optimisation, les défauts, erreurs ou abus constatés	Pas de communication possible ou souhaitée	Communication informelle au niveau des cadres supérieurs	Canal de communication formalisé, correspondant aux lignes de reporting habituelles d'une organisation	Voies de communication ouvertes et volontée affichée d'être à l'écoute	Mise en place de dispositifs encourageant la communication (formation du personnel, communication continue, mécanismes de feed-back), et même le signalement d'éventuelles violations du code de conduite.
6	Une communication adéquate sur la manière de l'organisation de gérer le risque est instaurée à l'externe (usagers, fournisseurs, autres organisations).	Pas de communication	Quelques discussions avec les usagers ou les fournisseurs par rapport à la manière dont l'entité gère les risques. Les risques sont rarement formalisés juridiquement dans la relation. Les risques sont plutôt considérés comme étant une affaire interne.	Discussions fréquentes avec les usagers et fournisseurs et bonne formalisation des risques dans les relations. Prise de conscience que la communication externe peut être importante pour améliorer le processus de gestion des risques.	Volonté déclarée de communiquer avec l'externe sur la manière dont l'organisation gère les risques.	La communication externe et la prise en compte des informations en résultant est incluse dans la politique des risques

VIII. SUIVI ET PILOTAGE

Le processus de management des risques est piloté dans sa globalité et modifié en fonction des besoins. Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités.

	Critères d'évaluation	N'existe pas	Existe mais n'est pas documenté	Existe de manière basique et documentée	Existe de manière développée et documentée	Existe de manière optimisée (stratégie et performance)
		1	2	3	4	5
1	Un dispositif de pilotage continu est en place afin que la direction soit assurée du bon fonctionnement du processus de gestion des risques, informée des défaillances et assurée que celles-ci soient traitées dans les meilleurs délais.	Pas de dispositif de pilotage	Le pilotage est assuré par la direction de manière informelle et sporadique	Le pilotage est assuré par la direction et les cadres supérieurs et est documenté dans un rapport ou PV	Des outils sont développés à différents niveaux de l'organisation pour s'assurer du bon fonctionnement de la gestion des risques et du traitement des défaillances dans les meilleurs délais.	Un dispositif évolué et continu de pilotage est intégré dans la politique de gestion des risques, il existe un reporting sur les défaillances du dispositif
2	Des évaluations spécifiques ponctuelles du processus de gestion des risques sont effectuées	Il n'y a pas de processus de gestion des risques	Il y a un processus de gestion des risques, mais il n'est jamais évalué	Le processus de gestion des risques est réévalué après des défaillances ou des modifications importantes dans l'organisation	Des évaluations du processus de gestion des risques ont lieu tous les 2 ou 3 ans afin de s'adapter au contexte interne de l'entreprise, elles peuvent ne concerner que certaines unités ou activités de l'organisation	Une évaluation globale du processus de gestion des risques ont lieu une fois par an, selon un processus d'évaluation déterminé, afin de s'adapter au contexte externe et interne de l'entreprise et à sa stratégie
3	Le risque résiduel est suivi	L'organisation n'a pas conscience qu'un niveau de risque résiduel est inhérent à son activité	L'organisation a conscience d'un niveau résiduel de risque associé à son activité, mais n'est pas en mesure de le quantifier	Le risque résiduel est réestimé après des défaillances ou des sinistres	Le risque résiduel est réestimé tous les 2 ou 3 ans	Le risque résiduel est réestimé tous les ans dans le cadre de la procédure d'évaluation de la gestion des risques

ANNEXE VI : DIRECTIVES SUR LA POLITIQUE DE GESTION DES RISQUES MENÉE PAR LA CONFÉDÉRATION

Directives sur la politique de gestion des risques menée par la Confédération

du 24 septembre 2010

Le Conseil fédéral suisse
édicte les directives suivantes:

1 Objet

[1] La politique de gestion des risques définit les conditions-cadres pour une gestion efficace et prévoyante des risques au sein de la Confédération.

[2] Elle constitue la base contraignante pour l'aménagement, la mise en œuvre, l'évaluation des prestations et l'amélioration de la gestion des risques.

[3] Les présentes directives fixent:

a. la définition du risque et le champ d'application des directives (ch. 2);
b. les buts de la gestion des risques (ch. 3);
c. les principes de la gestion des risques (ch. 4);
d. les fonctions en matière de gestion des risques (ch. 5).

2 Définition du risque et champ d'application des directives

[1] Par risques, on entend des événements et développements qui ont une certaine probabilité de se produire et qui ont des conséquences négatives majeures d'ordre financier et non financier sur l'atteinte des objectifs et l'exécution des tâches dans l'administration fédérale.

[2] Les présentes directives s'appliquent:

a. aux départements, aux secrétariats généraux et à la Chancellerie fédérale;
b. aux groupes et aux offices;
c. aux unités administratives de l'administration fédérale décentralisée qui n'ont pas de comptabilité propre.

3 Buts de la gestion des risques

[1] La gestion des risques vise à:[1]

a prévoir les événements et développements futurs et soutenir ainsi le Conseil fédéral et l'administration fédérale dans la prise de leurs décisions;

b. garantir la sécurité des représentants de la Confédération;

c. protéger le patrimoine et la réputation de la Confédération;

d. employer de manière efficace et économique les moyens à disposition.

[2] Pour atteindre les buts cités à l'al. 1, il convient:

a. d'inciter les collaborateurs à prendre conscience des risques;

b. d'identifier, analyser, évaluer et maîtriser les risques le plus tôt possible;

c. de prendre les mesures requises en se fondant sur l'exposition aux risques identifiée.

[3] La gestion des risques contribue ainsi:

a. à assurer une exécution prévoyante des tâches de la Confédération, et

b. à garantir le bon fonctionnement du gouvernement et de l'administration.

4 Principes de la gestion des risques

[1] La gestion des risques est un instrument de pilotage. Elle fait partie intégrante des processus de travail et de conduite et contribue à une exécution soigneuse et économe des tâches.[2]

[2] Les opérations d'identification, d'analyse, d'évaluation, de maîtrise et de surveillance des risques s'effectuent selon des règles uniformes. L'aménagement de la gestion des risques s'appuie sur les systèmes normatifs usuels.

[3] Une application informatique commune est mise en place dans l'administration fédérale pour la gestion des risques et l'établissement des rapports sur les risques.

[4] Les risques identifiés doivent dans toute la mesure du possible être évités ou atténués. Dans des cas particuliers, l'Administration fédérale des finances (AFF) peut autoriser la conclusion d'un contrat d'assurance pour transférer certains risques assurables.[3]

[5] Le Conseil fédéral, les départements, la Chancellerie fédérale ou les unités administratives décident et mettent en œuvre les mesures visant à éviter ou à atténuer les risques selon la situation et le niveau des risques concernés.

1 Cf. art. 39 de la loi du 7 octobre 2005 sur les finances de la Confédération (LFC; RS **611.0**).
2 Cf. art. 57, al. 1, LFC.
3 Cf. art. 50, al. 2 et 3, de l'ordonnance du 5 avril 2006 sur les finances de la Confédération (OFC; RS **611.01**) et les directives de l'AFF du 2 février 2009 applicables à la prise en charge des risques et au règlement des sinistres à la Confédération.

6 La gestion des risques comprend une gestion appropriée des urgences, des crises et de la continuité. Celle-ci traite les risques qui, malgré la prise de mesures, peuvent atteindre gravement et subitement une unité administrative. La gestion des risques tient compte des interfaces et interactions avec d'autres processus (p. ex. avec le système de contrôle interne).

7 Les résultats de la gestion des risques sont communiqués à l'interne et à l'externe de manière appropriée.

8 Le Conseil fédéral, les départements, la Chancellerie fédérale et l'AFF réexaminent régulièrement la politique de gestion des risques et veillent au développement et à l'amélioration de la gestion des risques.

5 Fonctions en matière de gestion des risques

1 La gestion des risques constitue un élément important du pilotage à tous les échelons.

2 La Conférence des secrétaires généraux (CSG) a notamment pour tâche:

a. de contrôler que les principaux risques des départements et de la Chancellerie fédérale soient identifiés et annoncés;

b. de consolider les risques transversaux;

c. de définir à l'attention du Conseil fédéral un ordre de priorité des risques selon les let. a et b.

3 L'AFF a notamment pour tâche:

a. de coordonner l'établissement des rapports et l'évaluation des prestations à l'attention de la CSG et du Conseil fédéral;

b. de mettre à disposition une seule et même application informatique pour la gestion des risques et l'établissement des rapports;

c. de veiller à ce que les responsables de la gestion des risques puissent bénéficier d'une formation adéquate;

d. d'encourager la mise en œuvre uniforme, le développement constant et l'amélioration de la gestion des risques au sein de la Confédération;

e. d'organiser régulièrement avec les responsables de la gestion des risques des départements et de la Chancellerie fédérale des séances de coordination concernant la gestion des risques et de permettre ainsi des échanges de vues entre les départements.

4 Les départements et la Chancellerie fédérale ont notamment pour tâche:

a. d'assumer la responsabilité des risques les concernant conjointement avec les propriétaires des risques. Ils bénéficient pour ce faire du soutien technique des responsables de la gestion des risques des départements et de la Chancellerie fédérale;

b. de mettre en œuvre la politique de gestion des risques conformément aux présentes directives et aux directives de l'AFF sur la gestion des risques et de mettre à disposition les ressources nécessaires;

c. de contrôler régulièrement et complètement leur exposition aux risques;

d. d'informer sans délai le Conseil fédéral sur toute situation de risque exceptionnelle et de le renseigner par ailleurs chaque année sur les risques dans leur domaine.

5 Les responsables des unités administratives ont notamment pour tâche:

a. d'assumer la responsabilité des risques les concernant conjointement avec les propriétaires des risques. Ils bénéficient pour ce faire du soutien technique du responsable de la gestion des risques de l'unité administrative;

b. de veiller au respect des directives de l'AFF ainsi qu'aux directives de leur propre département et de mettre à disposition les ressources nécessaires;

c. d'informer sans délai leur département sur toute situation de risque exceptionnelle et de le renseigner par ailleurs chaque année sur les risques dans leur domaine.

6 Dispositions finales

1 Après avoir consulté les responsables de la gestion des risques des départements et de la Chancellerie fédérale, l'AFF règle les modalités de la mise en œuvre dans des directives sur la gestion des risques.

2 Les présentes directives entrent en vigueur le 24 septembre 2010.

24 septembre 2010 Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Doris Leuthard
La chancelière de la Confédération, Corina Casanova

5968

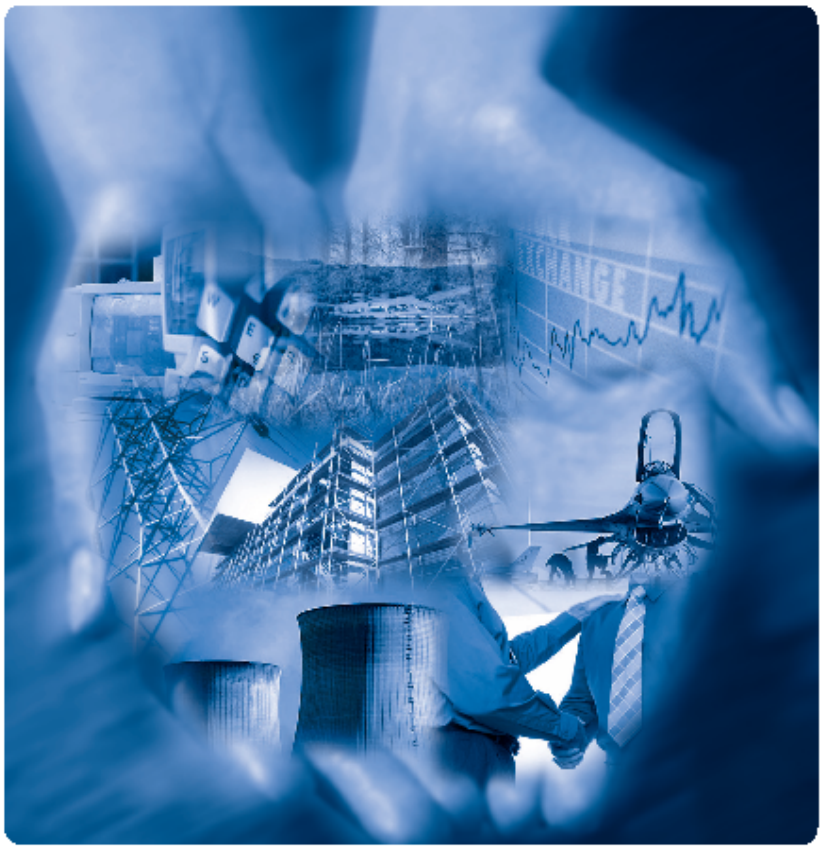
ANNEXE VII : POLITIQUE DE GESTION DES RISQUES AU SEIN DE LA CONFÉDÉRATION

www.efv.admin.ch

Politique de gestion des risques

Bases pour la gestion des risques au sein de la Confédération

Décembre 2004



Eidgenössisches Finanzdepartement EFD
Département fédéral des finances DFF
Dipartimento federale delle finanze DFF
Departament federal da finanzas DFF

TABLE DES MATIÈRES

1. Objet, buts et champ d'application de la politique de gestion des risques

1.1 Objet

La Confédération est exposée à divers risques. Elle est confrontée à de nouveaux défis: environnement de plus en plus interconnecté et complexe, efficacité accrue requise en matière de fourniture des prestations, gestion administrative responsable, diversité du catalogue des tâches de l'administration fédérale et restrictions budgétaires.

Focalisée sur les conséquences financières, la politique de gestion des risques pose les bases de la (⇒) **gestion des risques** au sein de la Confédération.

La politique de gestion des risques

- détermine une approche homogène et systématique des divers risques encourus au sein de l'administration fédérale,
- fait partie intégrante des obligations de diligence que les départements et les unités administratives doivent remplir dans le cadre de leurs activités,
- soutient les départements et les unités administratives dans l'exercice efficace de leurs tâches, et
- fournit des instruments et des mesures pour identifier, évaluer, maîtriser et surveiller les risques potentiels avec cohérence et efficacité.

1.2 Buts

Avec la politique de gestion des risques, le Conseil fédéral poursuit les buts suivants :

- exécution des tâches axées sur les résultats, la rentabilité et l'anticipation,
- maintien du bon fonctionnement de l'administration en tout temps,
- garantie d'un niveau élevé de sécurité physique pour les personnes et les valeurs patrimoniales,
- élimination maximale des cas de responsabilité civile,
- soutien des instances dirigeantes au moyen d'informations sur les risques complètes, transparentes et actualisées,
- conscience élevée des risques chez les collaborateurs de la Confédération,
- vue d'ensemble de la situation en matière de risques au niveau de la Confédération (y c. responsabilité en matière de couverture des déficits selon l'art. 19 de la loi sur la responsabilité [LRCF, RS 170.32]), des départements et des unités administratives,
- contrôle et réduction au minimum des coûts des risques[1] ,
- préservation de la bonne réputation de la Confédération en son propre sein, dans le public et vis-à-vis de ses autres interlocuteurs.

1.3 Champ d'application

En vertu du modèle des quatre cercles, le champ d'application de la politique de gestion des risques s'étend aux unités administratives des 1er et 2e cercles, soit à l'administration centrale et aux unités GMEB [2] .

Les organisations du 3e cercle et les entreprises du 4e cercle possèdent leurs propres politiques de gestion des risques. Les départements responsables de ces organisations et de ces entreprises s'assurent qu'elles disposent de leur propre gestion des risques.

2. Principes de maîtrise des risques

2.1 Stratégie de maîtrise des risques

Pour la maîtrise des risques, la Confédération applique les priorités suivantes:

- Evitement[3]
- Réduction
- Financement

Le volet «Financement» de la stratégie de maîtrise comprend l'auto-prise en charge et le transfert des risques. Cette stratégie concerne notamment les assurances.

2.2 Financement des risques

En règle générale, la Confédération assume les risques qu'elle encourt (principe de la prise en charge délibérée des risques).

La conclusion d'assurances peut toutefois s'avérer judicieuse dans certains cas exceptionnels, en particulier si les dommages potentiels s'élèvent à plus de 5 millions. Des détails se trouvent au chapitre 5, consacré à la politique d'assurance.

---

[1] Les coûts des risques comprennent les quatre éléments suivants:

- Coûts de prévention et coûts de limitation des dommages
- Coûts des dommages pris en charge par la Confédération
- Primes d'assurance et autres coûts résultant du transfert des risques
- Coûts administratifs

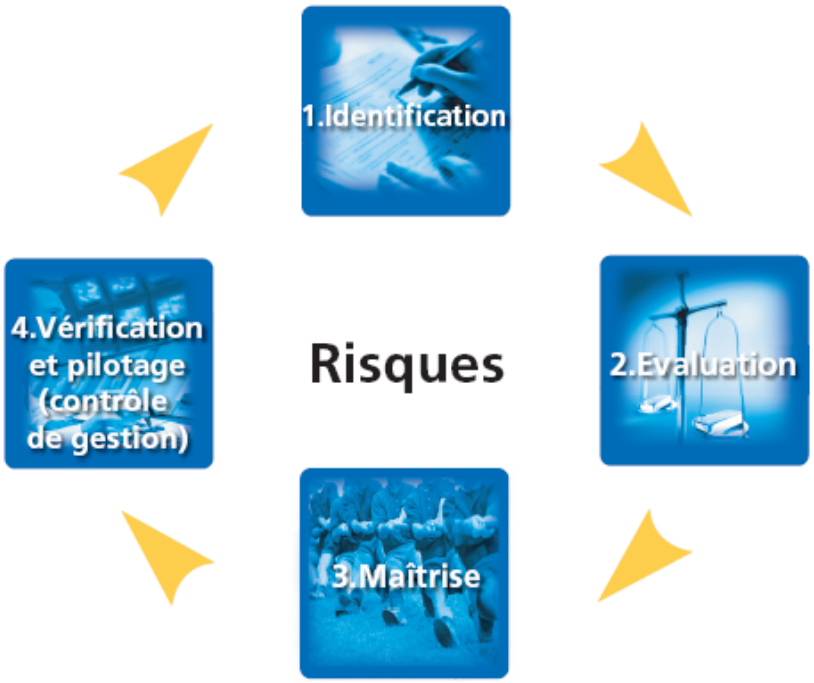
[2] GMEB signifie gestion par mandat de prestations et enveloppe budgétaire selon l'art. 44 LOGA et l'art. 38a LFC.

[3] Souvent, les risques ne peuvent pas être évités du fait de l'existence d'un mandat inscrit dans la loi.

3 Processus de gestion des risques

3.1 Vue d'ensemble

La mise en oeuvre de la gestion des risques au sein de la Confédération se déroule selon un processus standard. Il se compose des étapes illustrées ci-dessous:



Des solutions informatiques centralisées seront utilisées par l'administration fédérale pour mettre en oeuvre le processus de gestion des risques et soutenir les unités administratives.

1. **L'identification des risques** se fait de manière complète (voir chiffre 3.2).

2. Les risques sont ensuite évalués en fonction de leurs **conséquences financières et de la probabilité de leur occurrence**, puis classés par ordre de priorité (voir chiffre 3.3).

3. La troisième étape du processus de gestion des risques concerne **la maîtrise des risques**, basée sur l'évaluation de ces derniers. Les plans d'action constituent l'élément principal de la maîtrise des risques. Cette étape englobe la mise en oeuvre (voir chiffre 3.4).

4. Le processus s'achève avec le **contrôle de gestion des risques**. Il englobe la surveillance et le pilotage de la gestion des risques. Le processus étant continu, le contrôle de gestion des risques est suivi par l'identification de nouveaux risques (voir chiffre 3.5).

3.2 Identification des risques

L'identification des risques consiste en un inventaire complet et détaillé des risques. Elle se déroule du bas vers le haut de la hiérarchie, en d'autres termes, elle incombe aux unités administratives. Les risques répertoriés sont recensés dans des (⇒) **catalogues de risques** au niveau des départements, de la Chancellerie fédérale et de la Confédération.

L'identification des risques comprend deux phases: un premier «inventaire» à titre de document de base et une actualisation régulière (au moins 1 x par an) en vertu du processus continu et compte tenu de l'évolution des risques.

Les unités administratives des 1er et 2e cercles identifient aussi les risques résultant de la responsabilité en matière de couverture des déficits et d'autres garanties de la Confédération pour des organisations et entreprises des 3e et 4e cercles notamment, pour autant que la responsabilité de ces dernières incombe aux unités administratives.

Les risques, classés en fonction de leurs causes et de leurs conséquences, sont présentés de manière homogène. Les critères retenus pour la classification selon les causes sont les suivants:

- Risques financiers et économiques
- Risques juridiques et conformité «compliance»
- Risques matériels, techniques et élémentaires
- Risques liés aux personnes et à l'organisation
- Risques technologiques et scientifiques
- Risques sociaux et politiques

Les critères retenus pour la classification selon les conséquences se divisent en deux groupes:

- Conséquences financières :
    - Dommages corporels
    - Valeurs patrimoniales
    - Prétentions en dommages-intérêts
    - Prétentions non liées à la responsabilité civile

- Conséquences non financières :
    - Perturbation du fonctionnement du gouvernement et de l'administration
    - Atteinte à la réputation

L'annexe 2 contient un tableau de la (⇒) **matrice des risques** basée sur les critères de classement.

Pour l'identification des risques, les unités administratives utilisent des méthodes et des instruments courants comme l'analyse de documents, les entretiens, les inspections, les questionnaires, les techniques de scénario et les ateliers.

Les risques identifiés sont recensés dans un catalogue des risques[4] , présenté sous la forme de tableaux et contenant au moins les informations suivantes pour chaque risque répertorié:

- Unité administrative assumant le risque,
- Catégories de risques selon l'annexe 2,
- Description détaillée du risque,
- Scénarios critiques mais réalistes,
- Mesures de contrôle et de maîtrise existantes,
- Description des conséquences financières et non financières compte tenu des mesures de sécurité et de contrôle existantes.

Le catalogue des risques présente la situation en matière de risques de manière compréhensible pour les tiers. Il constitue la base pour l'évaluation des risques.

Exemple de catalogue des risques

Nr.	Unité administrative. Bref descriptif du risque («titre»)	Catégorie de risque (déterminée en fonction des critères «causes» et «conséquences»)	Définition du risque. Que pourrait-il se passer? Illustration à l'aide de scénarios réalistes	Mesures de maîtrise et de contrôle existantes: Qu'est-ce qui est déjà prévu actuellement?	Description des conséquences compte tenu des mesures déjà prises	
					financières	non financières
1						
2						
3						
4						
5						
6						
7						
Ff						

[4] L'«inventaire des risques de la Confédération suisse» contient les catalogues des risques issus de la première estimation effectuée en 2002.
Source: Rapport final de Kessler Consulting SA du 25 juin 2003.

3.3 Evaluation des risques

Chaque risque répertorié est évalué en fonction des deux critères suivants:

- Conséquences financières (importance du dommage potentiel)
- Probabilité d'occurrence

Une liste des risques (⇒) **liste des risques** et un profil des risques (⇒) **profil des risques** sont établis sur la base des évaluations.

Très souvent, la Confédération est exposée à des risques dont il est difficile de déterminer avec l'exactitude souhaitée l'importance des dommages potentiels et la probabilité d'occurrence. Les valeurs empiriques font souvent défaut. Des échelles sont donc utilisées pour évaluer les risques :

Echelles des risques

Conséquences financières en CHF	
Echelle	
1	< 10 000
2	10 000 – 1 million
3	1 – 10 millions
4	10 – 50 millions
5	50 – 100 millions
6	> 100 millions

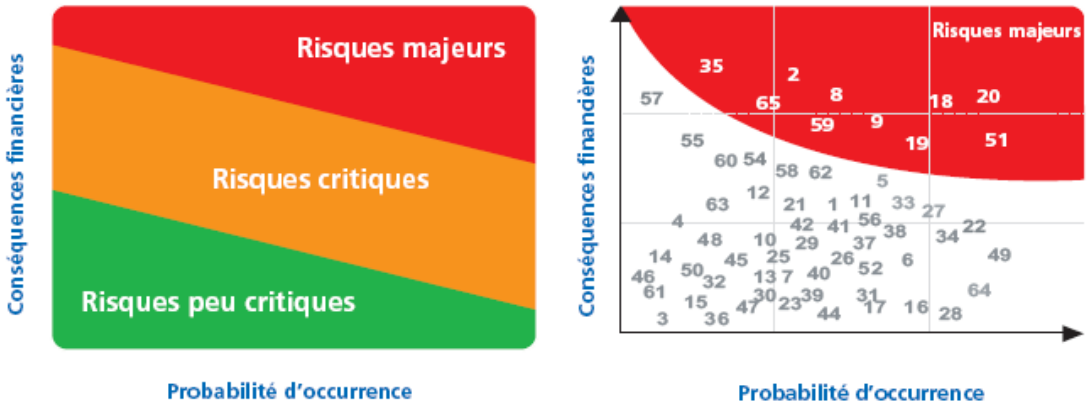
Probabilité d'occurrence dans	
Echelle	
1	> 10 ans
2	5 - 10 ans
3	3 - 5 ans
4	2 - 3 ans
5	1 - 2 ans
6	< 1 an

Une (⇒) **évaluation nette** est effectuée, tenant compte des mesures de sécurité et de contrôle existantes.

Les résultats de l'évaluation s'utilisent pour établir une liste des risques, classés par ordre d'importance. Cet ordre résulte de la multiplication des valeurs des deux échelles et indique l'importance des risques pour les unités administratives, les départements, la Chancellerie fédérale et la Confédération. Si elles sont importantes, les conséquences non financières constituent un critère subsidiaire pour le classement des risques. Il peut arriver qu'un risque gagne en importance dans la liste, suite à la prise en compte des conséquences non financières.

Les 10 risques figurant en tête de la liste des risques et les risques dont le montant des dommages potentiels dépasse 5 millions de francs constituent les (⇒) **risques majeurs** encourus par une unité administrative. En règle générale, ce sont les risques dont les conséquences financières potentielles sont élevées et/ou ceux qui présentent une probabilité d'occurrence supérieure à la moyenne. Les décideurs concernés doivent donc accorder une attention particulière aux risques majeurs.

Outre la liste par ordre d'importance, les risques sont aussi présentés sous la forme d'un nuage de points dans un système de coordonnées. Il s'agit du profil des risques. Chaque point représente un risque en fonction de sa probabilité d'occurrence et de l'ampleur des dommages potentiels. L'abscisse illustre la probabilité d'occurrence et l'ordonnée les conséquences financières.



Il est aussi possible de procéder à une (⇒) **agrégation des risques** en complément de l'évaluation des risques individuels. Cette méthode permet de déterminer l'exposition aux risques globaux.

Les départements et la Chancellerie fédérale sont libres de décider à quels services et quelles personnes ils confient, en leur sein, l'évaluation des risques. Ils doivent toutefois s'assurer que les risques sont analysés par des spécialistes possédant toutes les compétences requises[5] . Les départements, la Chancellerie fédérale et les unités administratives peuvent faire appel à des conseillers externes pour l'évaluation des risques. Ces conseillers accompagnent et soutiennent le processus. La responsabilité de l'évaluation ne peut toutefois pas leur être déléguée.

3.4 Maîtrise des risques

La maîtrise des risques se fonde sur l'identification et l'évaluation des risques. Elle consiste en la conception et la mise en oeuvre de mesures appropriées pour circonscrire les risques qui nécessitent une intervention (notamment les risques majeurs). Des plans d'action sont élaborés à cet effet pour les risques individuels ou liés.

Un (⇒) **plan d'action** se compose habituellement des points suivants (voir annexe 3):

- Caractérisation du risque
- Cause du risque

[5] En fonction du type de risque, d'autres méthodes (p. ex. des méthodes techniques ou basées sur les mathématiques financières) doivent pouvoir être utilisées pour une évaluation plus détaillée.

- Evaluation financière du risque ne tenant pas compte des mesures de sécurité et de contrôle existantes
- Mesures de sécurité et de contrôle existantes
- Indicateurs financiers et non financiers pour la détection précoce et le contrôle de l'évolution du risque dans le temps
- Description de l'évolution du risque dans le temps
- Processus administratifs concernés
- Conséquences non financières
- Evaluation financière du risque tenant compte des mesures de sécurité et de contrôle existantes
- Demande éventuelle d'une solution d'assurance à l'Administration fédérale des finances
- Description des mesures à prendre et des ressources nécessaires

Chaque plan d'action doit être signé par le (⇒) **responsable assumant le risque**.

Les mesures prévues doivent réduire au minimum la probabilité d'occurrence et/ou les conséquences financières et non financières du risque concerné. La même importance sera accordée aux mesures agissant sur les causes (prévention) qu'aux mesures agissant sur les conséquences (limitation des dommages).

Des critères organisationnels, techniques, liés au personnel, contractuels et financiers doivent entrer en ligne de compte lors de l'élaboration des mesures visant à prévenir, diminuer et financer les risques.

3.5 Contrôle de gestion des risques

Le contrôle de gestion des risques comprend la surveillance et le pilotage du processus de gestion des risques. Il assure la continuité et l'amélioration du processus conformément aux principes de la politique de gestion des risques. Le contrôle de gestion des risques met en évidence les écarts par rapport aux objectifs de la politique de gestion des risques. Il sert en outre à évaluer les effets des mesures.

Les rapports constituent un élément important du contrôle de gestion des risques. Ce dernier suppose un système fonctionnel et uniforme de rapports et de documentation, basés sur des informations actuelles et objectives.

Dans le cadre des rapports ordinaires, le contrôle de gestion des risques s'appuie sur les documents et rapports suivants :

- Le catalogue des risques
- La liste des risques
- Le profil des risques
- Les plans d'action
- La statistique des dommages

Ces documents sont élaborés à l'échelon des unités administratives, puis transmis aux départements.

Dans le cadre du rapport de gestion, le Conseil fédéral s'appuie sur ces informations pour s'exprimer au sujet de la politique de gestion des risques et ce, en ce qui concerne la Confédération dans la partie générale et les départements dans la partie spéciale. Le rapport de gestion porte notamment sur l'évolution des risques et l'état d'avancement des plans d'action. Il présente aussi une vue d'ensemble de la situation en matière d'assurance.

Outre les activités de rapport ordinaires, les unités administratives doivent signaler sans tarder les évolutions extraordinaires des risques et/ou les dommages.

Les unités administratives disposent d'un système de gestion des crises pour les cas où un événement d'une portée particulière est annoncé ou survient.

La détection précoce des situations potentiellement critiques est un élément essentiel du contrôle de gestion des risques. Dans les unités administratives, les responsables de la gestion des risques définissent à cet effet, au moyen d'indicateurs, des domaines d'observation spécifiques.

Dans le cadre du contrôle périodique du respect de la stratégie de propriétaire, les départements veillent à ce que les institutions, organisations et entreprises des 3e et 4e cercles qui leur sont subordonnées appliquent des mesures appropriées de gestion des risques.

La gestion des risques de la Confédération doit être développée en permanence et se conformer aux standards de qualité en vigueur sur le marché. Dans cette perspective, il est nécessaire d'examiner régulièrement et d'un œil critique l'adéquation, la faisabilité, l'efficacité et la fiabilité des procédures de travail ainsi que les méthodes et instruments utilisés et au besoin de les adapter.

4. Responsabilité

La responsabilité de la politique de gestion des risques est assumée par:

- Le Conseil fédéral
- Les départements et la Chancellerie fédérale
- Les unités administratives
- Les responsables assumant les risques dans les unités administratives

4.1 Conseil fédéral

Le Conseil fédéral assume la haute responsabilité de la gestion des risques au sein de la Confédération.

4.2 Départements et Chancellerie fédérale

Les départements et la Chancellerie fédérale assument la responsabilité des risques dans leur domaine de compétence. Ils s'assurent que le processus de gestion des risques a été mis en place et s'utilise régulièrement dans les unités administratives des départements et à la Chancellerie fédérale.

Il incombe également aux départements de veiller à ce que leurs unités administratives tiennent compte des risques encourus, dans le cadre de la responsabilité en matière de couverture des déficits selon l'art. 19 LRCF, par les organisations leur étant subordonnées. Ce principe concerne aussi les organisations pour lesquelles la Confédération assume d'autres garanties.

4.3 Unités administratives

Les unités administratives assument une responsabilité directe conformément aux dispositions de la politique de la Confédération en matière de gestion des risques. Il leur incombe de mettre en œuvre le processus de gestion des risques dans le cadre de leurs activités administratives.

Les unités administratives sont responsables de l'identification et de l'évaluation des risques et de l'élaboration des plans d'action. Elles surveillent les progrès de la mise en oeuvre des mesures et veillent à l'optimisation de la situation en matière de risques. Elles s'assurent que les informations liées aux risques soient rassemblées et transmises à leurs départements.

Pour les risques importants, des responsables sont désignés dans les unités administratives. Leur domaine de compétence et de responsabilité comprend l'identification, l'analyse et la gestion active (détection précoce incluse) des risques ainsi que la conduite, en cas de besoin, d'un système de gestion des crises. Ils veillent à ce que la situation en matière de crise s'améliore en permanence. Les responsables assumant les risques sont des spécialistes[6] des risques ou des cadres dont ils s'occupent. Cette fonction peut donc être assumée par le responsable d'une unité administrative.

Les responsables de risques comparables survenant dans plusieurs unités administratives s'accordent pour tirer profit des synergies. Au besoin, les unités administratives peuvent faire appel à des externes pour des analyses approfondies.

Elles veillent à offrir une formation et un perfectionnement adéquats en matière de gestion des risques pour garantir le bon déroulement des tâches qui leur sont confiées.

5. Politique d'assurance

5.1 Réglementation des compétences

L'Administration fédérale des finances (AFF) définit[7] et met en oeuvre la politique de la Confédération en matière d'assurance, qui fait partie intégrante de la politique de gestion des risques. L'AFF

- édicte des instructions sur l'auto-prise en charge, l'assurance des risques et le règlement des sinistres et fixe la procédure administrative interne,
- décide de la conclusion ou de la non-conclusion de contrats d'assurance, un contrat d'assurance n'étant conclu qu'en accord avec le responsable du risque,
- conclut les contrats d'assurance pour l'ensemble de l'administration fédérale (1er et 2e cercles),

[6] Exemple de spécialistes: préposé à la sécurité, responsable des finances, juriste, responsable technique, responsable administratif.

[7] Art. 43a de l'ordonnance sur les finances de la Confédération (RS 611.01).

- lance des appels d'offre OMC,
- définit les critères pour la conclusion de contrats d'assurance et les adapte en fonction de l'évolution de la situation,
- fournit aux unités administratives une liste permettant de déterminer si un risque répertorié peut être assuré,
- gère les polices d'assurance,
- contrôle et optimise régulièrement, en collaboration avec l'OFPER, les conditions de contrat des assurances de personnes dont les primes sont prises en charge par la Confédération,
- étudie conjointement avec les services spécialisés les questions d'assurance liées à de grands projets d'acquisition et de construction,
- suit le règlement des sinistres assurés et
- se procure, par le biais d'un système de déclaration, une vue d'ensemble de l'ampleur et des causes des sinistres touchant la Confédération (dommages aux valeurs patrimoniales d'une part, dommages en responsabilité civile d'autre part).

5.2 Conclusion d'assurances

En vertu du principe selon lequel la Confédération assume les risques qu'elle encourt, les solutions d'assurance prescrites par des lois ou des ordonnances doivent être supprimées dans la mesure du possible.

Les dommages potentiels dépassant la barre des 5 millions de francs peuvent faire l'objet d'un contrat d'assurance après examen du rapport coûts-bénéfices. Les solutions d'assurance choisies doivent dans la mesure du possible être valables pour l'ensemble de l'administration fédérale.

Lorsqu'une activité de la Confédération ne peut être exercée qu'après conclusion d'une assurance de droit privé, le contrat doit être conclu si l'unité administrative responsable décide que l'activité en question doit se poursuivre.

La conclusion et la gestion d'assurances obligatoires à l'étranger incombent aux représentations suisses et aux bureaux de coopération situés dans les pays concernés. En ce qui concerne les assurances non obligatoires, l'AFF peut leur déléguer ses compétences.

La conclusion d'un contrat de règlement des sinistres avec une compagnie d'assurance compétente en la matière doit être examinée lorsque le règlement des sinistres occasionne une lourde charge administrative ou s'il se déroule dans une mesure considérable à l'étranger.

6. Financement

Les départements et la Chancellerie fédérale remplissent les tâches liées à la politique de gestion des risques avec les moyens mis à leur disposition.

En principe, les primes d'assurance sont inscrites de manière décentralisée au budget des unités administratives responsables de la gestion des risques concernés.

Les dommages non assurés jusqu'à hauteur de 10 000 francs sont financés par des moyens budgétisés par l'Administration fédérale des finances. Les moyens pour financer les dommages non assurés supérieurs à ce montant font l'objet d'une demande des départements dans le cadre du budget et du supplément au budget.

Annexe 1 : Lexique de la politique de gestion des risques

Gestion des risques	La gestion des risques constitue le cadre d'une approche planifiée des risques encourus par la Confédération. La gestion des risques découle de la politique de gestion des risques. Elle englobe l'identification, l'évaluation, la maîtrise et le contrôle de gestion des risques.
Catalogue des risques	Inventaire des risques classés selon des critères tels que les causes et les conséquences. Le catalogue des risques énumère par ailleurs les mesures déjà prises et décrit les évolutions possibles.
Matrice des risques	Présentation des risques et de leurs causes sous la forme d'un tableau. Les risques sont classés par catégories et par domaines d'influence (financiers et non financiers).
Liste des risques	Classement des risques en fonction de leur gravité. Les risques préalablement évalués sont présentés dans un ordre d'importance décroissant.
Profil des risques	Graphique bidimensionnel du paysage des risques. La probabilité d'occurrence est illustrée par l'abscisse, tandis que l'ordonnée se réfère au montant des dommages. Chaque point du graphique représente un risque. Le nuage de points constitue le paysage des risques (illustration globale des risques).
Evaluation brute et nette	L'évaluation brute des risques ne tient pas compte des mesures de sécurité et de contrôle existantes. L'évaluation nette tient compte de ces mesures.
Risques majeurs	On entend par risques majeurs les dix premiers risques de la liste et ceux dont le montant des dommages potentiels est supérieur à 5 millions de francs, encourus par une unité administrative, un département, la Chancellerie fédérale ou la Confédération. Les risques majeurs se caractérisent généralement par des conséquences financières potentielles élevées et/ou par une probabilité d'occurrence supérieure à la moyenne.
Agrégation des risques	L'agrégation des risques représente l'exposition globale aux risques compte tenu des interactions entre les risques majeurs. Le profil des risques individuels porte au contraire sur leurs positions relatives. L'agrégation des risques peut par exemple s'effectuer en utilisant des simulations de type Monte-Carlo (recours à des scénarios).

Plan d'action	Instrument de travail pour la maîtrise des risques. Il présente notamment les manières de prévenir ou de réduire la probabilité d'occurrence d'un risque et /ou le montant des dommages.
Responsable assumant le risque	La responsabilité de chaque risque incombe à une personne au sein du département ou de l'unité administrative concernée. Cette personne assume la responsabilité opérationnelle des risques dont elle doit s'occuper.

Annexe 2: matrice des risques

Catégories de risques		Domaines d'influence au sein de l'administration fédérale					
		financiers				non financiers	
	Explication et exemples (liste non exhaustive)	Diminution des patrimoniales	Dommages corporels	Prétentions en dommages-intérêts	Autres prétentions (non liées à la responsabilité civile)	Perturbation du fonctionnement de l'administration	Atteinte à la réputation
Risques financiers et économiques	Risques liés à la gestion des finances, à la dépendance économique de la Confédération vis-à-vis de tiers ou à des prestations subsidiaires de la Confédération · variations des taux d'intérêts · fournisseurs et partenaires · prêts, cautionnements et garanties · participations de la Confédération (p. ex. Swisscom ou Swiss) · assistance de la Confédération lors d'événements majeurs ou de catastrophes à l'étranger (p. ex. incident nucléaire, attentat terroriste, intempéries, tremblement de terre)						
Risques juridiques et observation de la loi	Risques liés à l'exécution des tâches administratives et au respect des dispositions et contrats juridiques · violation du devoir de surveillance et d'information · responsabilité relative au patrimoine de la Confédération (p. ex. entreprises, bâtiments, véhicules) · responsabilité en matière de couverture de déficits selon l'art. 19 LRCF · responsabilité pour les organes, pour les membres des autorités et les employés de la Confédération · responsabilité fondée sur la confiance · violation de contrat						
Risques matériels et techniques	Risques liés à la destruction ou l'endommagement de bâtiments, établissements, installations techniques, données ou biens culturels appartenant à la Confédération – interruptions de service incluses · incendies de bâtiments appartenant à la Confédération · explosions de halles de stockage pour produits dangereux · inondations · pannes informatiques						
Risques liés aux personnes et à l'organisation	Risques liés aux personnes dans les domaines de l'organisation, de la direction, du personnel et de la protection des personnes · embauche de spécialistes et planification de la relève · gestion de projet et gestion du savoir · absences · abus de confiance · accidents de visiteurs						
Risques technologiques / scientifiques	Risques liés au développement, à l'autorisation et au lancement de nouvelles applications technologiques / scientifiques (y compris risques ultérieurs) · rayons non ionisants (télécommunication) · génie génétique · technologie nucléaire						
Risques sociaux / politiques	Risques liés à l'environnement social / au système politique · méconnaissance des évolutions sociales · décisions politiques (modification de la loi / constitution)						

Annexe 3: Modèle de plan d'action

1. Caractérisation des risques
2. Processus administratifs concernés
3. Causes du risque
4. Indicateurs financiers et non financiers
5. Evaluation du risque financier sans tenir compte des mesures existantes
6. Conséquences non financières
7. Mesures existantes
8. Evaluation du risque financier en tenant compte des mesures existantes
9. Description du développement du risque dans le temps
10. Description des mesures à prendre, ressources nécessaires incluses
11. Demande d'une solution d'assurance à l'AFF
12. Signataire assumant le risque

ANNEXE VIII : LA COUR DES COMPTES EN BREF

La Cour des comptes du canton de Vaud a pour mission d'assurer en toute indépendance le contrôle de la gestion des finances des institutions publiques désignées par la LCComptes du 21 novembre 2006 ainsi que l'utilisation de tout argent public sous l'angle de la légalité, de la régularité comptable et de l'efficacité (art. 2 LCComptes).

Les **attributions** de la Cour sont les suivantes (art. 24 LCComptes) :

- contrôle de l'utilisation de tout argent public ;
- contrôle de la gestion financière, notamment sous l'angle du principe d'efficience, ainsi que vérification de l'évaluation de la gestion des risques des entités soumises à son champ de contrôle ;
- examen des investissements qui bénéficient de subventions, prêts ou garanties de l'Etat.

La Cour **se saisit elle-même** des objets qu'elle entend traiter à l'exception des mandats qui lui sont attribués par le Grand Conseil Vaudois, sur requête de la majorité des députés (art. 25 et ss LCComptes).

Sont soumis au contrôle de la Cour (art. 28 LCComptes):

- le Grand Conseil et son Secrétariat général ;
- le Conseil d'Etat, ses départements et ses services ;
- le Tribunal cantonal ainsi que les tribunaux et autres offices qui lui sont rattachés ;
- les communes, ainsi que les ententes, associations, fédérations et agglomérations de communes ;
- les corporations, établissements, associations, fondations, sociétés et autres entités auxquels le canton ou une commune confie des tâches publiques ;
- les corporations, établissements, associations, fondations, sociétés et autres entités auxquels le canton ou une commune apporte un soutien financier, que ce soit par des subventions, des aides financières ou des indemnités ou pour lesquels il constitue des cautionnements ou des garanties.

Les rapports de la Cour consignent ses constatations et recommandations (art. 36 LCComptes). Ils comprennent également les observations de l'entité auditée, les éventuelles remarques subséquentes de la Cour et, le cas échéant, les avis minoritaires de la Cour.

La Cour **publie ses rapports** pour autant qu'aucun intérêt prépondérant, public ou privé, ne s'y oppose. Ils sont consultables sur le site internet de la Cour : www.vd.ch/cdc.

Vous pouvez apporter votre contribution au bon usage de l'argent public en contactant la Cour des comptes. Toute personne peut communiquer à la Cour des signalements en rapport avec des faits entrant dans ses attributions. Il suffit de vous adresser à :

Cour des comptes du canton de Vaud
Rue de Langallerie 11, 1014 Lausanne
Téléphone : +41 (0) 21 316 58 00 Fax : +41 (0) 21 316 58 01
Courriel : info.cour-des-comptes@vd.ch