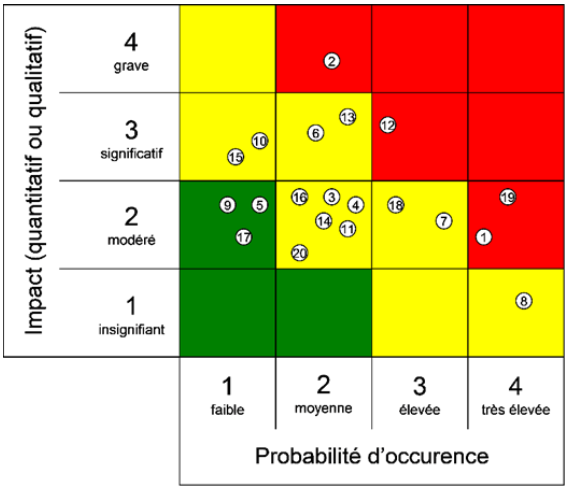
COUR DES COMPTES
CANTON DE VAUD

Cour des comptes du canton de Vaud

Audit de la gestion intégrée des risques

Analyse comparative dans six entités de l'administration cantonale vaudoise



Rapport n° 81

Rue Langallerie 11 - 1014 Lausanne
Téléphone : 021 316 58 00
info.cour-des-comptes@vd.ch

Une synthèse de ce rapport et une capsule vidéo de présentation des travaux d'audit sont librement accessibles sur la page Internet de la Cour des comptes du canton de Vaud : www.vd.ch/cdc.

Vous trouverez également sur ce site des informations générales sur les attributions, le fonctionnement et le champ de contrôle de la Cour des comptes.

Table des matières

Les termes en *italique* dans le rapport figurent dans le glossaire (annexe II)

1. Contexte et objectifs de l'audit

1.1. Pourquoi un audit sur la gestion des risques ?

Une mission spécifique de la Cour des comptes

La Cour a décidé de lancer un audit sur la vérification de l'évaluation de la *gestion des risques* (GDR) en vertu d'une mission qui lui est spécifiquement confiée par la loi :

> **Art. 4 al. 2 LCComptes**
> La Cour des comptes procède à la vérification de l'évaluation de la gestion des risques des entités soumises à son champ de contrôle.

Pour pouvoir remplir cette mission, deux prérequis sont nécessaires : l'existence d'une GDR et son évaluation régulière. Comme indiqué dans l'Exposé des motifs du projet de loi sur la Cour des comptes[1] (p. 42), la Cour 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 mis en place par l'entité pour gérer les risques de ses activités.

Depuis sa création en 2008, la Cour des comptes a publié deux audits sur la GDR :

- **Analyse comparative dans huit musées cantonaux et communaux, Rapport n° 11** (2010) : L'objectif de cette mission était d'évaluer le processus de GDR mis en place par huit musées relativement importants (trois musées cantonaux et cinq musées communaux). Il en ressortait que les musées disposaient d'un système de gestion des risques de conservation et de sécurité, mais non intégré et partiellement formalisé.
- **Analyse comparative dans cinq entités de l'administration cantonale vaudoise (ACV), Rapport n° 27** (2013) : Les services audités étaient le Secrétariat général de l'ordre judiciaire vaudois, la Division asile et retour du Service de la population, le Service des automobiles et de la navigation, le Service de la protection et de la jeunesse et le Service pénitentiaire. L'audit a conclu que les entités prenaient en compte les risques dans leurs pratiques quotidiennes, mais ne disposaient cependant pas d'une approche intégrée des risques. La Cour a donc recommandé la mise en place d'une *gestion intégrée des risques* pour l'ensemble de l'ACV et de certains éléments qui lui sont essentiels (p.ex. fixation d'objectifs SMART, inventaire des risques, système d'information et de communication y relatif).

La Cour des comptes a mis fin au suivi de ce dernier rapport en 2018. Le Conseil d'Etat (CE) entendait dans un premier temps concentrer ses efforts sur l'implémentation du *système de contrôle interne* (SCI) financier. Depuis lors, le SCI financier a progressivement été déployé au sein de l'ACV, avec une certification en 2023 des derniers services par le Contrôle cantonal des finances (CCF). La Cour a ainsi jugé opportun de relancer un audit sur la GDR, en conformité avec sa mission légale.

[1] EMPL sur la Cour des comptes n° 344 de juin 2006

1.2. La gestion intégrée des risques

Définitions

La gestion des risques

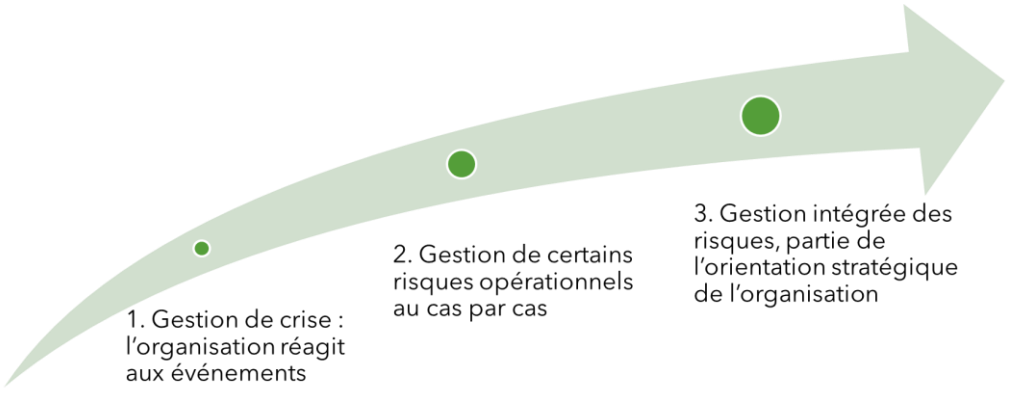
Le risque est l'effet de l'incertitude sur les objectifs. Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces.[2]

La GDR constitue un instrument important de pilotage à tous les échelons d'une organisation, qui s'appuie sur des systèmes normatifs usuels. Il s'agit d'un ensemble de pratiques visant à anticiper les événements futurs et à soutenir la prise de décisions. Elle fait partie intégrante des processus de travail et de conduite et contribue à une exécution soigneuse et économe des tâches. Les opérations d'identification, d'analyse, d'évaluation, de maîtrise et de surveillance des risques s'effectuent selon des règles uniformes.[3]

Des mesures pour gérer les risques sont prises en fonction du contexte et du niveau de risque. La GDR ne vise pas à éviter tous les risques, mais permet aux organisations de prendre des décisions éclairées grâce à une compréhension de leurs risques et, en fin de compte, de réagir en atténuant les menaces et en tirant profit des opportunités. La GDR englobe également la gestion des urgences, des crises et de la continuité, en tenant compte des interactions avec d'autres processus et en favorisant le développement continu de ses pratiques.

De la gestion de crise à une gestion intégrée des risques

La capacité à anticiper, évaluer et traiter les risques de manière économe, efficiente et efficace varie considérablement d'une organisation à l'autre. La GDR évolue progressivement, en trois étapes, passant de la gestion de crise à une *gestion intégrée des risques*[4] :



1. **La gestion de crise :** L'organisation réagit aux événements qui perturbent la réalisation de ses objectifs en ajustant ses actions a posteriori. Cette approche peut entraîner des coûts élevés, des solutions inefficaces et des risques pour la réputation de l'organisation.

[2] ISO 31073:2022, art. 3.1.1
[3] Basé sur les Directives sur la politique de gestion des risques menée par la Confédération du 24 septembre 2010
[4] Rapport CdC n° 27 de 2013

2. **La gestion de certains risques opérationnels au cas par cas :** Les risques sont identifiés et évalués de manière individuelle, p.ex. lors d'un nouveau projet de construction ou de l'implémentation d'un programme informatique. Cependant, tous les risques ne sont pas couverts et la GDR n'est pas intégrée dans un processus global aligné sur les objectifs de l'organisation et son appétence aux risques.
3. **La *gestion intégrée des risques*, partie de l'orientation stratégique de l'organisation :** L'organisation adopte « 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 »[5]. Cette approche fait partie intégrante de la stratégie de l'organisation et contribue à la réalisation de ses objectifs. Elle nécessite une évaluation continue des risques à tous les niveaux, une vision globale des risques et des priorités, ainsi qu'une culture interne tournée vers la GDR.

Une intégration sur trois plans

La GDR intégrée repose sur trois types d'intégration :

1. **Intégration fonctionnelle :** La GDR est intégrée en tant qu'instrument de conduite, avec une prise en compte systématique des risques par tous les échelons hiérarchiques dans tous les processus et activités de l'organisation. Cela inclut la planification, la définition de la stratégie et la gestion de changements importants.
2. **Intégration verticale :** Les informations circulent de manière fluide entre tous les niveaux hiérarchiques. Les instructions et les objectifs sont transmis de haut en bas pour garantir une mise en œuvre homogène. Grâce à son expertise pratique, l'échelon opérationnel identifie et remonte les risques importants. Les décisions prises à chaque niveau tiennent compte des risques pertinents. Cela permet au niveau supérieur de se concentrer sur les risques prioritaires et de limiter son portefeuille de risques.
3. **Intégration horizontale :** La GDR est mise en réseau avec les autres processus d'aide à la conduite, tels que la gestion financière, le pilotage informatique et le *système de contrôle interne*. Une coordination efficace entre ces processus assure une utilisation cohérente des ressources et une GDR harmonisée. Les risques interdépendants et transversaux sont ainsi pris en compte et gérés de manière coordonnée. Cela nécessite d'établir des mécanismes de communication et de collaboration efficaces entre les différentes parties prenantes impliquées dans la GDR.

Ces trois principes d'intégration permettent une gestion globale et cohérente des risques, garantissant ainsi une prise de décision éclairée et une utilisation efficace des ressources.

La gestion des risques dans le secteur public

Le secteur public est confronté à un environnement complexe et à des attentes multiples. Or l'incertitude est source de risques et d'opportunités, susceptibles de détruire ou de créer de la valeur, et par conséquent de servir plus ou moins bien l'intérêt public. Afin de relever ces défis, la direction de chaque entité publique doit déterminer un degré d'incertitude acceptable pour réaliser sa mission et ses objectifs.

[5] Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, mai 2016

L'Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques (INTOSAI) a émis des lignes directrices pour guider la GDR des entités publiques. Notamment la norme GOV 9130 (voir annexe V), qui se base sur le modèle *COSO II* (voir chapitre 1.4.), fait partie des normes de bonne gouvernance de l'INTOSAI. Cette norme encourage les entités à identifier les risques et les opportunités, à préciser leurs objectifs et à élaborer des contrôles internes pour minimiser les risques et maximiser les opportunités. Elle stipule que la GDR doit être un processus continu, intégré à tous les niveaux et unités de l'organisation, et doit permettre d'anticiper les événements pouvant affecter la réalisation des objectifs.

De nombreuses administrations publiques, telles que la Confédération (voir annexe IV), l'Etat de Genève[6], le Canton de Berne[7], les administrations publiques canadienne[8], française[9] ou encore anglaise[10], ont mis en place un système de *gestion intégrée des risques*. Elles se basent généralement sur des référentiels reconnus internationalement, tels que le *COSO* déjà mentionné, l'*ISO 31000* ou encore la norme ÖNORM D 4901 qui s'appuie sur *ISO 31000* (voir annexe V). Ces initiatives démontrent l'importance accordée à la GDR dans le secteur public, en vue d'une gestion efficace et d'une amélioration de la performance organisationnelle.

Les organisations qui n'accordent pas suffisamment d'attention à la mise en place d'un cadre pour la *gestion intégrée des risques* peuvent se retrouver avec des solutions fragmentées, où chaque service développe sa propre approche de GDR. Il peut en résulter un manque de cohérence et une utilisation inefficace de l'argent public.

Intérêt et valeur ajoutée de la gestion intégrée des risques

Une *gestion intégrée des risques,* mise en œuvre de manière performante, présente de nombreux avantages. En particulier, elle peut :

- Améliorer l'exécution des politiques publiques et soutenir de façon prospective l'accomplissement des tâches et l'atteinte des objectifs ;
- Faciliter l'établissement de priorités et permettre de prendre des décisions de manière éclairée et proactive, en tenant compte d'événements et de développements potentiels ;
- Permettre de mieux se préparer aux situations d'urgence ou de crise, de réduire l'impact de ces situations et d'améliorer la continuité des activités ;
- Assurer une allocation efficiente et efficace des ressources humaines, financières et matérielles disponibles ;
- Inciter les collaborateur·trice·s à prendre conscience des *risques inhérents* à leur domaine d'activité ;
- Accroître la transparence et la vue d'ensemble de la situation en matière de risques ;

[6] Règlement sur la gestion des risques du 18 septembre 2013.
[7] Directives sur la gestion des risques du Canton de Berne du 24 novembre 2021.
[8] Guide de la gestion intégrée des risques du Secrétariat du Conseil du Trésor du Canada, mai 2016
[9] 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.
[10] The Orange Book, Management of Risk - Principles and Concepts, HM Treasury, October 2004.

- Contribuer à renforcer la confiance des parties prenantes envers les autorités et l'administration, en communiquant clairement sur les risques et les choix effectués.

Il est important de noter que la GDR ne vise pas à supprimer la totalité des risques, qui font partie de toute activité, mais à aider l'organisation à les évaluer, les traiter et à prendre en compte, dans un système formel, les effets positifs (opportunités) en plus des impacts négatifs.

1.3. Les objectifs et le périmètre de l'audit

Les objectifs de l'audit

L'audit avait pour objectif de répondre à la question suivante :

Une gestion intégrée des risques est-elle mise en œuvre dans l'administration cantonale vaudoise ?

Consciente dès le lancement du présent audit qu'aucune instruction générale n'avait encore été donnée par le CE pour l'ensemble de l'ACV, la Cour a fixé les objectifs complémentaires suivants :

- Faire un état des lieux de la GDR en examinant les pratiques d'une sélection de services ;
- Evaluer la sensibilité à l'importance d'une *gestion intégrée des risques* au sein des services audités.

Les questions d'audit permettant de remplir ces objectifs sont issues de la méthodologie de la Cour spécifique aux audits de vérification de l'évaluation de la GDR et étaient basées sur les cinq composantes du modèle *COSO-ERM 2017*. Les outils d'analyse (voir chapitre 1.4. pour la description du questionnaire et de la matrice de maturité) ont été mis à jour pour tenir compte de l'évolution du cadre *COSO* depuis le dernier audit sur la GDR mené en 2013 (voir chapitre 1.1.).

Cet audit n'avait pas pour but d'évaluer les risques des services, cette tâche leur étant réservée.

Le périmètre de l'audit

Pour des raisons d'exemplarité et de capacité d'audit de la Cour, un échantillon de six services a été sélectionné sur la base des critères suivants :

- Deux services déjà inclus dans l'audit de 2013 sur la *gestion intégrée des risques* :
  - Le Service des automobiles et de la navigation (SAN), qui dépend du DCIRH
  - Le Service pénitentiaire (SPEN), qui dépend du DJES.
- Deux directions avec un budget et un nombre d'ETP d'importance significative :
  - La Direction générale de l'emploi et du marché du travail (DGEM), qui dépend du DEIEP
  - La Direction générale de l'enseignement postobligatoire (DGEP), qui dépend du DEF
- Deux entités transversales :
  - Le Secrétariat général du Département des institutions, du territoire et du sport (DITS)
  - La Chancellerie d'Etat (CHA)

Entité auditée	Budget 2023 — charges	Budget 2023 — revenus	Budget 2023 — ETP	
SAN	35'646'300	351'030'900	221.20	
SPEN	151'314'800	27'667'800	628.44	
DGEM	125'428'400	103'520'500	47.60	[11]
DGEP	620'385'200	120'855'800	3'108.08	[12]
SG-DITS	7'147'700	1'188'700	31.25	
CHA	16'561'700	411'200	51.30	[13]

La sélection a également tenu compte des services ayant récemment fait l'objet d'un audit de la Cour, ainsi que d'une représentation de différents départements.

1.4. L'approche et la méthode d'audit

Les modèles de référence COSO

Evolution de COSO II à COSO-ERM 2017

Lors de l'audit de 2013 sur la *gestion intégrée des risques*, la Cour a utilisé un modèle basé sur le cadre *COSO II*, modèle officiel établi par le *Committee of Parrainage Organizations of the Treadway Commission* et retenu par INTOSAI (voir chapitre 1.2.). Pour répondre aux défis posés par les incertitudes croissantes, les modèles économiques complexes, les exigences en matière de responsabilité et de reporting, le *COSO* a actualisé le cadre de référence du management des risques. Cette révision a abouti à la publication du *COSO-ERM 2017*, qui représente la version actualisée et améliorée du cadre précédent.

En résumé, cette mise à jour apporte plusieurs améliorations, elle :

- Clarifie l'importance du management des risques lors de l'élaboration et la mise en œuvre de la stratégie ;
- Renforce l'articulation entre la performance et le management des risques ;
- Prend en compte les attentes en matière de gouvernance et de surveillance ;
- Reconnaît la mondialisation des marchés et des activités ;
- Propose de nouvelles approches pour appréhender les risques dans un contexte plus complexe ;
- Elargit le reporting pour plus de transparence ;
- S'adapte aux évolutions technologiques et à l'abondance des données et des analyses nécessaires pour étayer la prise de décisions ;
- Fournit des définitions et des principes pour chaque niveau de management impliqué.

[11] Selon la brochure budget 2023 de l'Etat de Vaud : Les collaboratrices et collaborateurs de la DIPP, de la CCh, et de la DIACE ne sont pas inclus dans ces données salariales. A fin avril 2022, la DGEM employait un total de 576 personnes représentant 543.30 ETP.
[12] Centrale DGEP 251.30 ETP + Etablissements enseignement secondaire II 2'856.777 ETP.
[13] N'inclut pas les sept postes de Conseiller·ère·s d'Etat élu·e·s.

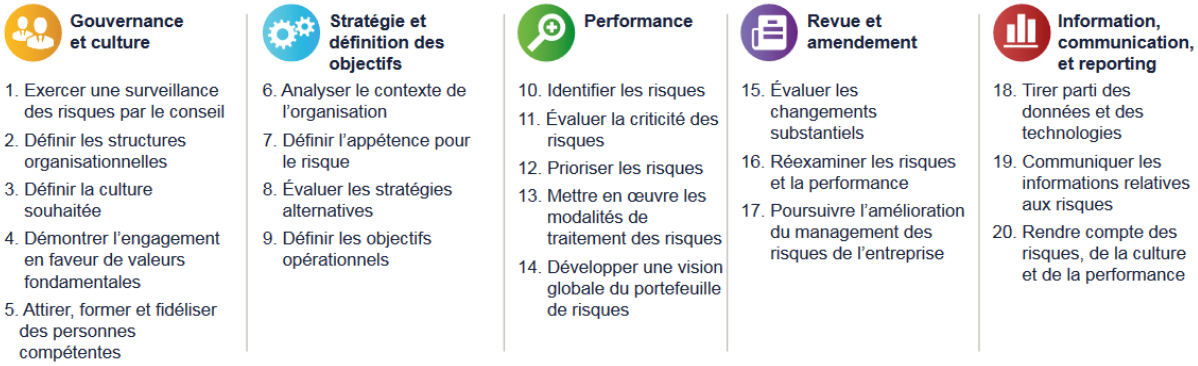
COSO-ERM 2017

Le nouveau cadre de référence s'articule à présent autour de cinq composantes indépendantes qui s'adaptent à différentes structures organisationnelles pour soutenir la stratégie et la prise de décision :

1. Gouvernance et culture
2. Stratégie et définition des objectifs
3. Performance
4. Revue et amendement
5. Information, communication et reporting

Sa représentation graphique souligne que la maîtrise des risques est intégrée au cycle de management et de pilotage de l'organisation :

Les cinq composantes ci-dessus se subdivisent en vingt principes couvrant divers aspects, allant de la gouvernance au pilotage. Ces principes, adaptés à des organisations de tailles, types et secteurs variés, établissent des pratiques applicables. En les adoptant, la direction peut raisonnablement attendre que l'organisation développe une compréhension approfondie des risques liés à sa stratégie et à ses objectifs opérationnels, et s'engage dans leur gestion proactive.



Source des deux figures ci-dessus : Le management des risques de l'entreprise — Une démarche intégrée à la stratégie et à la performance – Synthèse, COSO, juin 2017

Des détails supplémentaires sur ce modèle sont disponibles dans une publication traduite en français par l'Institut français de l'audit et du contrôle internes (voir annexe V).

La méthode d'évaluation de la gestion des risques

Mise à jour du questionnaire de la Cour selon COSO-ERM 2017

Les cinq composantes et vingt principes du modèle de *gestion intégrée des risques COSO-ERM 2017* (voir ci-dessus) ont été évalués spécifiquement par le biais d'un questionnaire (voir Annexe VI) et d'un modèle de maturité (voir Annexe VII).

Pour ce faire, la Cour a revu le questionnaire et la matrice de maturité, qui avaient été développés pour les audits de 2010 et 2013, afin de les rendre compatibles avec le nouveau modèle *COSO-ERM 2017*.

Evaluation des réponses

Dans le souci d'examiner les pratiques en matière de GDR au sein de l'Etat, la Cour a procédé à l'évaluation individuelle de chaque composante et principe, indépendamment de son intégration dans un système de gestion globale des risques.

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

Niveau de maturité du système de gestion des risques	Critères d'évaluation
1 **Inexistant ou peu fiable**	L'élément considéré est inexistant dans l'organisation ou n'est pas appliqué.
2 **Informel, limité**	L'élément considéré existe dans l'organisation, mais de manière peu développée et peu ou pas documentée.
3 **Standardisé**	L'élément considéré existe dans l'organisation, il est documenté de manière basique, connu et appliqué.
4 **Surveillé, évalué**	L'élément considéré existe de manière développée et documentée.
5 **Optimisé, intégré**	L'élément considéré est optimisé au sein d'un système de *gestion intégrée des risques*.

La Cour considère que le niveau à partir duquel on peut admettre que l'organisation a atteint un degré de maturité jugé comme satisfaisant en l'état actuel est le **niveau 3 — standardisé**.

Ce type de notations figurent aussi dans la directive n° 22 du SAGEFI sur le SCI financier (voir chapitre 2.1.2.) et le CE demande aux entités d'atteindre au minimum le niveau d'exigence n° 3 standardisé.

Comme en 2013, en raison de l'absence de cadre cantonal (contraignant ou même recommandé), la Cour estime pertinent de ne pas inclure dans ce rapport les notations individuelles des entités auditées. Le but est de tirer des constatations de portée générale et des recommandations applicables à l'ensemble de l'administration cantonale à partir de l'échantillon observé. La Cour a en revanche restitué à chaque service audité les analyses, constats et recommandations spécifiques à leur domaine d'activité.

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 ce sens, qui méritent d'être exposés (voir chapitre 2.2).

COSO un modèle parmi d'autres

Le modèle COSO a été sélectionné pour les audits de gestion des risques, car c'est celui reconnu par les normes INTOSAI qui servent de base à tous les audits menés par la Cour des comptes. Cette approche garantit une cohérence et une conformité aux normes internationales dans l'évaluation de la GDR au sein de l'ACV.

Cependant, la Cour souligne que l'ACV ne doit pas nécessairement se référer au cadre COSO pour mettre en œuvre un système de gestion des risques intégré. L'ACV peut en effet adopter d'autres modèles ou normes pertinents, en fonction de ses besoins spécifiques. Il existe plusieurs normes de référence alternatives dans ce domaine, dont des exemples sont fournis dans l'annexe V du rapport.

L'approche d'audit

L'annexe III renseigne sur les axes d'analyse retenus et les procédures d'audit menées.

Le processus d'élaboration du rapport a été le suivant :

- Les constatations et recommandations préliminaires ont été présentées le 22 juin 2023 à la DGEP, le 26 juin 2023 au SPEN, le 7 juillet 2023 à la CHA, le 10 juillet 2023 au SAN et au SG-DITS et le 20 juillet 2023 à la DGEM. Une séance a également eu lieu le 13 juillet 2023 avec une délégation du Conseil d'Etat.

- Un avant-projet de rapport a été adressé simultanément aux différentes entités auditées, ainsi qu'au Conseil d'Etat, en date du 3 octobre 2023.

- Le projet de rapport a été adressé au Conseil d'Etat et aux entités auditées le 2 novembre 2023 afin qu'ils puissent formuler leurs remarques (délai de 21 jours). Ces remarques sont reproduites au chapitre 5 du présent rapport.

- Le Collège des magistrat·e·s délibérant en séance plénière en date du 5 décembre 2023 a adopté le rapport public en présence de Madame Valérie Schwaar, présidente, Madame Nathalie Jaquerod et Monsieur Guy-Philippe Bolay, vice-président·e·s.

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. Elle formule ainsi 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.

Remerciements

La Cour des comptes tient à remercier toutes les personnes qui lui ont permis de réaliser cet audit. Elle souligne la disponibilité de ses interlocuteur·trice·s, la qualité des échanges 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 aux directions, collaboratrices et collaborateurs des six entités auditées :

- Service des automobiles et de la navigation (SAN) ;
- Service pénitentiaire (SPEN) ;
- Direction générale de l'emploi et du marché du travail (DGEM) ;
- Direction générale de l'enseignement postobligatoire (DGEP) ;
- Secrétariat général du Département des institutions, du territoire et du sport (SG-DITS).
- Chancellerie d'Etat (CHA) ;

Plusieurs responsables dans les entités auditées ont relevé que, vu l'absence de directives cantonales en la matière, le manque de système formalisé de GDR aurait certainement aussi été constaté en choisissant d'autres entités. La Cour tient d'autant plus à les remercier d'avoir pleinement participé aux démarches d'audit.

2. Résultats de l'audit

2.1. Evolution de la situation dans l'ACV depuis 2013

2.1.1. Un cadre cantonal toujours inexistant

La situation concernant l'évaluation des risques du Canton de Vaud n'a pas évolué depuis 2013, à savoir qu'il n'existe toujours aucune exigence ou directive spécifique en la matière dans la réglementation cantonale en vigueur.

Convaincue que la GDR est un élément essentiel d'une bonne gouvernance des institutions publiques et en accord avec sa mission légale (art. 4 al. 1 let. b LCComptes), la Cour avait émis les recommandations suivantes lors de ses audits de 2010 et 2013 :

- « 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, audit n° 11 de 2010).
- « Une approche de *gestion des risques* commune pour l'Etat de Vaud doit être définie au sein d'une politique de *gestion des risques* » (recommandation n° 2, audit n° 27 de 2013).

En tant qu'organe de contrôle indépendant, la Cour des comptes entendait ainsi encourager le Canton de Vaud à prendre en compte la GDR dans ses pratiques et à mettre en place un cadre de référence pour une *gestion intégrée des risques* au sein de l'ACV. Cet objectif reste pleinement valable actuellement.

2.1.2. Démarches lancées ces dernières années

La Cour relève que le Canton n'a toutefois pas été inactif dans ce domaine ces dernières années. Plusieurs projets transversaux ont été lancés ou finalisés et constituent les premiers jalons d'une *gestion intégrée des risques*.

Un système de contrôle interne financier mis en place et certifié

L'ensemble des services de l'administration vaudoise ont dû mettre en place un *système de contrôle interne* (SCI) financier conformément à la directive d'exécution n° 22 sur le SCI, émise en 2010 et mise à jour en 2022. Cette directive fournit un cadre méthodologique englobant toutes les procédures et mesures organisationnelles destinées à assurer un travail efficace et à minimiser les risques et erreurs dans les états financiers. Elle se réfère à l'art. 16, al. 1, let. e LFin qui ne traite du SCI que sous l'angle de l'application de la loi sur les finances et non pas sur toutes les dispositions légales ou réglementaires qui régissent les missions des services proprement dites.

Le délai initial pour la mise en place du SCI était fixé au 1er janvier 2016, mais le processus a été ralenti, notamment par l'arrivée du nouveau système d'information financier (SAP). Ce projet de longue haleine a finalement abouti en 2023. Dans ce cadre, tous les services ont réalisé une *cartographie de leurs risques* financiers, voire de certains risques de conformité. Ainsi, dans son rapport sur l'audit des comptes annuels de l'Etat de Vaud pour l'exercice arrêté au 31 décembre 2022, le CCF a pu supprimer

la réserve et attester, pour la première fois, qu'il existait un SCI relatif à l'établissement des comptes annuels, qui atteignait le niveau 3 tel que défini dans la directive d'exécution n° 22.

Le Contrôle cantonal des finances (CCF) a pour responsabilité d'attester de l'existence du SCI. De 2009 à 2023, il a réalisé la certification initiale de chaque service de l'ACV. Cependant, à ce jour, le CCF n'a pas procédé à un suivi régulier de l'évolution ou du maintien du SCI des services après leur certification. Il est désormais nécessaire d'inclure une revue périodique du SCI dans le cadre de la révision annuelle des comptes. Dans le rapport de la COFIN de juin 2023 sur les comptes 2022, il est d'ailleurs mentionné que le CCF souligne l'importance de maintenir à jour le SCI, en particulier en intégrant les nouvelles missions et les risques des services.

La mise en place du SCI est certes une première étape dans la formalisation de la GDR au sein du Canton de Vaud, mais celle-ci ne doit toutefois pas se borner uniquement aux risques financiers et de conformité. D'autres aspects tels que les risques opérationnels et stratégiques doivent également être pris en compte pour une approche globale et intégrée de la GDR.

Politique générale de sécurité des systèmes d'information et analyse des risques de sécurité informatique

En 2011, l'Etat de Vaud a mis en place une Politique générale de sécurité des systèmes d'information (PGSSI-VD[14]) et des plans directeurs[15] pour guider ses initiatives futures en matière de systèmes d'information. Le Plan directeur cantonal des systèmes d'information vise à développer un environnement numérique responsable, sécurisé et innovant, mettant l'accent sur la sécurité avec les personnes, le contrôle d'accès, l'architecture de sécurité et la réponse aux incidents de sécurité.

Depuis 2013, l'Etat de Vaud a réalisé des avancées significatives en matière de gestion des risques liés aux systèmes d'information et aux technologies. Après avoir obtenu la certification *ISO 9001* en 2018, la Direction générale du numérique et des systèmes d'information (DGNSI) a décroché début 2023 la certification ISO 27001, témoignant de la mise en place de systèmes de gestion de la qualité et de la sécurité conformes aux meilleures pratiques internationales en ce qui concerne la GDR.

Pour rappel, un premier projet (EMPD n° 61 d'avril 2013) a permis de « mener une analyse des risques complète, de mettre en place un certain nombre de mesures de diminution des risques, de mettre en service un centre de sécurité opérationnel, d'instaurer un système de management de la sécurité de l'information (SMSI) et d'équiper un centre informatique de secours en cas de catastrophe pour un nombre limité d'applications critiques »[16].

Un deuxième projet (EMPD n° 147 de juin 2019), impliquant un investissement de CHF 9'506'000 étalé sur cinq ans, vise à renforcer la sécurité de l'information au sein de l'ACV. Il s'inscrit dans la continuité des travaux précédents en se focalisant sur quatre axes prioritaires : la sécurité avec les personnes, le contrôle d'accès, l'architecture de sécurité et la réponse aux incidents de sécurité. Il est considéré comme un prérequis pour les futures évolutions des systèmes d'information, notamment en matière

[14] Actuellement en vigueur : Version 1.5 du 26.10.2022

[15] Actuellement en vigueur : Plan directeur cantonal des systèmes d'information 2018-2023, version 1.11 du 04.02.2019

[16] Source : EMPD n° 147 de juin 2019, promulgué le 4 février 2020

de sécurité, en lien avec l'avènement de la société numérique, et intégrant en particulier la sécurité des objets connectés.

La Cour a publié précédemment deux rapports en lien avec cette thématique, portant sur la gouvernance des projets de système d'information métier (rapport n° 67 de juillet 2021) et sur la protection des données personnelles (rapport n° 74 de décembre 2021).)

Gestion intégrée des risques naturels

Ces dernières années, les catastrophes naturelles ont causé d'importants dommages dans le canton de Vaud, remettant en question la politique de gestion des dangers naturels. Afin de mieux faire face à ces dangers, les autorités et leurs partenaires ont adopté une approche de « culture du risque » en mettant en place une *gestion intégrée des risques* naturels.

Cette nouvelle approche se fonde sur des mesures préventives pour réduire la vulnérabilité des personnes et des biens, ainsi que sur des actions de maîtrise des événements pour limiter l'ampleur des sinistres et assurer la reconstruction après un événement. La *gestion intégrée des risques* permet un lien systémique entre la prévention, la maîtrise et la reconstruction et elle est alimentée par l'évaluation des dangers et des risques à partir d'expériences vécues lors de catastrophes. Elle implique la collaboration de nombreux acteurs, tels que les spécialistes des dangers naturels, les services d'aménagement du territoire, les assurances, les services d'alerte, les forces d'intervention, ainsi que les particuliers.

En 2014, le Canton a émis des directives[17] et mis à disposition une documentation générale sur les dangers naturels pour une meilleure *gestion intégrée des risques*. Des guides pratiques et des fiches d'application sont fournis pour faciliter l'évaluation des risques dans les projets de planification. Un catalogue[18] de cette documentation présente les produits et outils disponibles. Une Unité des dangers naturels (UDN) est en charge de la prévention et de la protection des personnes et des biens contre les dangers et les catastrophes d'origine naturelle.

Un nouveau guichet cartographique professionnel est également mis à disposition, permettant l'accès aux données géospatiales relatives aux dangers naturels. De nouvelles cartes indicatives de dangers sont disponibles pour informer sur les zones exposées. De plus, la participation de la population est encouragée via un cadastre des événements. Grâce à ces ressources et à une approche concertée, le Canton de Vaud s'efforce de mieux prévenir et gérer les risques liés aux catastrophes naturelles, assurant ainsi la sécurité et le bien-être de ses citoyen·ne·s.

Analyse des risques pour la protection de la population

En décembre 2021, après trois ans de travaux, le CE a adopté le rapport sur l'analyse des risques pour la protection de la population. Cette étude visait à mieux connaître et réduire les dangers auxquels la population est exposée. Elle a identifié 12 principaux dangers menaçant la population du canton de

[17] Directives cantonales du 18 juin 2014 exposant comment intégrer les dangers naturels dans la planification du territoire et Directive cantonale du 30 octobre 2019 fixant le principe des standards & objectifs cantonaux de protection (SOP)

[18] Catalogue de la documentation sur les dangers naturels, DGE-DIRNA-UDN, 08.11.2021 https://www.vd.ch/fileadmin/user_upload/themes/territoire/dangers_naturels/fichiers_pdf/2021_Catalogue_de_la_documentation_sur_les_dangers_naturels.pdf

Vaud, par exemple les sécheresses, les épidémies et pandémies, les pannes d'électricité, les précipitations violentes et les vagues de chaleur. La plupart d'entre eux montrent une nette tendance à la hausse, en raison notamment du changement climatique.

En évaluant les risques, cette analyse alimente les réflexions sur les mesures de prévention et de préparation, tout en se nourrissant des retours d'expérience lors de sinistres ou d'exercices. Elle est une condition préalable pour apprécier les capacités opérationnelles des partenaires et élaborer des stratégies et plans d'action pour réduire les risques auxquels la population vaudoise est exposée.

Il est essentiel de souligner que cette analyse présente une image de la situation à un moment précis et n'est pas une prédiction. Ainsi, une veille permanente et une révision régulière sont indispensables afin de maintenir une vision pertinente au fil du temps et d'adapter les mesures pour protéger au mieux la population face aux risques identifiés.

Le CE prévoit de mettre à jour cette analyse tous les cinq ans pour adapter les mesures de réduction des risques. Une brochure de synthèse du rapport du CE sur l'analyse des risques a été publiée[19], fournissant des informations essentielles sur les principaux dangers, la gestion intégrale des risques et les contacts utiles.

Gestion de la crise COVID

En 2020, l'ACV a élaboré des plans de continuité liés à la pandémie de COVID-19. Ces plans visaient à maintenir l'activité au niveau le plus élevé possible malgré les perturbations causées par la crise sanitaire. Ils comprenaient des mesures pour permettre le télétravail, offrir une protection maximale à tout le personnel de l'ACV, adapter les procédures opérationnelles et garantir la communication avec le public. Le but était d'assurer, dans tous les cas, la continuité des tâches essentielles par l'affectation anticipée de moyens adéquats.

Les plans de continuité ont été conçus de manière à être flexibles et à s'adapter aux évolutions de la situation épidémiologique, afin de mieux faire face aux défis rencontrés lors de la pandémie.

Chaque service a passé en revue l'ensemble de ses processus afin de désigner un·e responsable et un·e suppléant·e, indiquer si le télétravail était possible pour l'activité en question et définir les niveaux de priorité en cas de crise sanitaire, selon la liste suivante :

1. Activités absolument indispensables, toutes les ressources sont nécessaires, voire plus ;
2. Activités pouvant être réduites en partie, mais certaines prestations devant être maintenues, une majorité des ressources est nécessaire ;
3. Activités pouvant être réduites à leur strict minimum, une majorité des ressources peut être réallouée ;
4. Activités pouvant être suspendues pendant plusieurs semaines, les ressources peuvent être réallouées.

[19] Synthèse – Rapport du Conseil d'Etat, 2021 – Analyse des risques – Protection de la population, Département de l'environnement et de la sécurité, Service de la sécurité civile et militaire, Publié en avril 2022. https://www.vd.ch/fileadmin/user_upload/themes/securite/protection_population/fichiers_pdf/Analyse_des_risques/220406_02_03_CG_Brochure_synthe%CC%80se_12p_VF.pdf

Plan de continuité en cas de pénurie énergétique

Une stratégie cantonale a été adoptée, à l'automne 2022, pour faire face au risque de pénurie d'électricité et de gaz dans les prochaines années, renforcé par des éléments incontrôlables tels que la géopolitique et la météo. Elle vise à promouvoir des économies d'énergie dans l'ACV et les bâtiments publics, à encourager des comportements économes chez la population, les entreprises et les communes et à garantir la continuité des prestations essentielles en cas de pénurie, notamment dans les domaines de la santé, de la sécurité, de la fourniture en eau potable ou de biens de première nécessité.

En 2022, les services de l'ACV ont adapté les plans mentionnés ci-dessus afin d'assurer une continuité des activités en cas de pénurie énergétique. Ces plans n'ont heureusement pas dû être mis en œuvre durant l'hiver 2022-23, mais les importants travaux de préparation et d'analyse effectués permettent de disposer d'une base solide et d'établir une feuille de route en prévision des hivers prochains.

2.2. Analyse des résultats des six entités auditées

Comme indiqué au chapitre 1.4, la Cour a décidé de ne pas inclure dans ce rapport les notations individuelles attribuées aux différents éléments du questionnaire pour chacune des six entités auditées. Cette décision a été motivée par l'absence de cadre cantonal en matière de GDR et la volonté de ne pas cibler spécifiquement les entités auditées par rapport au reste de l'ACV. Dans le cadre de l'audit, la Cour a néanmoins pu constater que les activités des entités auditées tenaient généralement compte des risques, à des degrés toutefois très divers. Le chapitre 2.2 vise ainsi à présenter les principaux constats et relever les bonnes pratiques observées. La Cour a pris le parti d'adresser uniquement des recommandations au Conseil d'Etat dans le but d'instaurer une *gestion intégrée des risques* au sein de l'ensemble de l'ACV.

Les résultats sont présentés de manière condensée, en trois groupes :

- Les deux services ayant déjà été audités en 2013 ;
- Les deux directions générales regroupant de multiples entités ;
- Les deux services transversaux qui jouent un rôle de coordination.

Cette approche permet aussi de mettre en évidence les problèmes découlant de l'absence de cadre cantonal et justifiant d'adresser des recommandations globales au CE, car elles concernent l'ensemble de l'ACV (voir chapitre 3).

Comme cela a été observé en 2013, les entités prennent en compte les risques dans leurs pratiques quotidiennes, malgré l'absence d'un référentiel de GDR à l'échelle de l'ACV. La direction des services a une bonne perception des risques directement liés à leurs prestations, principalement les risques opérationnels. Même si un système de *gestion intégrée des risques* basé sur un référentiel reconnu (tel que *COSO* ou ISO) n'a pas encore été mis en place, la Cour a pu constater, dans ses démarches auprès des services, que certaines procédures sont déjà formalisées. Des dispositions favorables existent, néanmoins les risques ne sont pas systématiquement abordés ni nécessairement liés aux objectifs. Un niveau de maturité élevé dans la GDR est toutefois observé pour certains services qui ont obtenu une certification (par exemple, *ISO 9001:2015* ou qualité).

2.2.1. Services déjà audités en 2013

Le SAN et le SPEN ont déjà à l'heure actuelle un système de GDR d'un niveau de maturité élevé, avec des notations supérieures au niveau 3 « standardisé » (considéré comme satisfaisant) pour l'ensemble des composantes *COSO*.

De bonnes pratiques développées par ces services sont exposées ci-après pour illustrer des exemples d'approches proactives de la GDR.

Service des automobiles et de la navigation (SAN)

Culture de la qualité

Le SAN fonctionne selon une approche « management par objectifs », avec des processus formalisés et un suivi de la qualité des prestations. Des objectifs sont fixés annuellement et déclinés jusqu'au niveau individuel. Chaque collaborateur·trice dispose d'un cahier des charges remis à jour régulièrement et différents autres documents apportent des précisions (matrices de compétences, fil rouge décrivant comment réaliser les prestations, intranet, planification annuelle, mensuelle et journalière, notes et procédures, etc.).

Le service réalise une planification annuelle pour gérer efficacement la charge de travail. Cela permet de mieux répartir les tâches, de faire face aux fluctuations saisonnières et d'éviter le risque de sur ou sous-occupation.

Ressources humaines

Le SAN a publié une charte comportant les valeurs et règles de vie qui engagent l'ensemble du personnel, cadres et membres de la direction. Celles-ci sont présentées aux personnes nouvellement embauchées dans le cadre de journées d'accueil. Le service promeut une forte culture axée sur la qualité avec diverses initiatives favorisant la participation et la sensibilisation du personnel. Le service prend des mesures préventives ciblées pour gérer certains risques, notamment en menant régulièrement des enquêtes de satisfaction auprès du personnel et en mettant en place des mesures visant à améliorer le bien-être au travail et à réduire l'absentéisme. De plus, une plateforme informatique permet aux membres du personnel d'annoncer des risques ou des problèmes rencontrés, et de faire des propositions d'amélioration.

Le SAN dispose d'une politique de formation et de relève. Il veille également au développement des compétences de son personnel en adéquation avec l'évolution du cadre légal et des exigences de sa clientèle. Des formations continues internes sont données aux collaborateur·trice·s dans les domaines métier. Les cadres suivent automatiquement une formation managériale en relation avec leur niveau de compétences. Une revue des compétences est effectuée lors des entretiens de suivi et de développement.

Outils de communication interne

Les droits d'accès aux systèmes sont définis en fonction des compétences et de la sensibilité des données. Par exemple : seuls les collaborateur·trice·s des mesures administratives ont accès aux données concernant les retraits de permis de conduire.

Le SAN juge l'outil métier utilisé VIACAR performant, mais ce n'est pas à proprement parler un outil de GDR. Il ne génère notamment pas d'alerte s'il y a des conflits d'utilisation des pistes de contrôle de

véhicules (2 expertises programmées sur le même poste) ou si l'expert ne dispose pas du bon profil (certains sont spécialisés pour des types de véhicules). Le SAN indique que ces fonctionnalités pourraient être ajoutées dans la future version de cette plateforme.

L'Observatoire clientèle permet à l'ensemble du personnel de faire des suggestions d'amélioration (SA) ou de communiquer des non-conformités (NC) constatées, afin d'alimenter le processus d'amélioration continue. Lorsqu'une demande doit être prise en charge, le comité qualité l'attribue à une personne qui reçoit une alerte par courriel. Tout est suivi dans cette plateforme et la responsable qualité envoie des rappels pour les objets non traités. Dans tous les cas, la personne qui a émis la SA/NC est informée du traitement de sa demande. Par ailleurs, une plateforme informatique permet à tout le personnel du SAN de faire part de problèmes de logistique ou liés aux bâtiments, et de requérir une intervention ou réparation (p.ex. fuite d'eau, néon à remplacer). Toutes les demandes de ce type sont ainsi documentées et peuvent être suivies jusqu'à leur résolution.

Interactions intercantonales
Le SAN est membre de deux associations soit l'asa (Association des services des automobiles) et la vks (Association des services cantonaux de la navigation). Ces deux associations édictent des normes et assurent également un rôle de soutien, voire de surveillance dans certains cas sur délégation de l'OFROU et l'OFT. La Division Technique du SAN procède notamment, tout au long de l'année, à différents contrôles demandés par la Conférence des chefs latins des services des automobiles.

Enquêtes et contrôles
Chaque année depuis 2009, une enquête de satisfaction clientèle est réalisée par un organisme externe. Cette démarche permet non seulement de faire un benchmark avec les services similaires des autres cantons romands, mais aussi de tracer l'évolution du résultat de certains indicateurs. Les résultats montrent une tendance positive.

Les résultats du SAN sont examinés régulièrement au moyen d'indicateurs sur les activités, notamment lors de réunions mensuelles du comité de direction. Cette approche permet de surveiller les performances du service et d'identifier les éventuels risques émergents. Lors de la revue annuelle par la direction, tous les processus sont passés en revue avec un examen des forces et des faiblesses. Un plan d'amélioration continue (PAC) – contenant plusieurs mesures – peut ainsi être mis en place pour remédier aux défauts constatés ; ce PAC est suivi régulièrement par le comité de direction. Au terme de la revue de direction, un document est publié sur intranet, dans un objectif de transparence, pour tout le personnel.

Le SAN a également introduit des audits croisés pour renforcer les efforts d'amélioration continue. Ces audits, réalisés par des collaborateur·trice·s formé·e·s à l'audit, permettent d'identifier les problèmes de conformité et les faiblesses. De plus, des contrôles aléatoires sont effectués par chaque division et documentés dans un tableau de suivi, pour détecter les éventuelles fraudes et renforcer la sécurité des procédures.

Par ailleurs, des contrôles sont effectués par un mandataire externe au moyen d'un « véhicule fantôme » qui présente des défauts, afin de mesurer l'expertise métier lors des contrôles techniques ainsi que l'accueil des client·e·s.

Certifications

Le SAN est certifié selon les normes *ISO 9001:2005* depuis 2011 (actuellement *ISO 9001:2015*). La nouvelle version de cette norme met l'accent sur la prévention et exige un management des risques, autrement dit une approche par les « risques et opportunités » ainsi qu'un suivi lors de la revue de direction annuelle, coordonnée par la responsable qualité.

La norme *ISO 9001:2015* exige que l'organisme comprenne son contexte, détermine les risques et planifie les actions pour y faire face. Elle prévoit notamment une revue annuelle du contexte, de la matrice des risques, de la matrice des tâches/collaborateur·trice qui liste aussi les suppléances et du plan de formation. Ces éléments couvrent les éléments essentiels de ce qui est attendu d'un système de GDR.

Le SAN a également obtenu les certifications ISO 17020 depuis 2014 et système qualité asaSAQ pour les contrôles techniques des véhicules. Les processus sont documentés et soumis à un audit de suivi annuel ainsi qu'à un audit de re-certification tous les trois ans par un organisme externe.

Les audits de suivi, de surveillance et de ré-accréditation ou de re-certifications ont toujours été réussis depuis dix ans. Malgré l'absence d'une approche formalisée pour la GDR à l'échelle de l'ensemble de l'ACV, le SAN a développé une culture de la qualité et déployé des démarches visant à obtenir et à maintenir les certifications ISO qui ont abouti à l'instauration d'un niveau élevé de GDR au sein du service.

Service pénitentiaire (SPEN)

Culture axée sur la sécurité

Le SPEN travaille au quotidien avec des personnes détenues présentant de nombreux risques, notamment : violences physiques et verbales, mutinerie, prise d'otage, trafic de stupéfiants, introduction d'objets interdits, acte d'automutilation voire suicide, fuite, péjoration de la santé liée à la privation de liberté, endoctrinement et sectarisme, etc.

L'activité du SPEN implique des risques non seulement pour les personnes détenues, mais également pour la sécurité publique ainsi que pour les collaboratrices et collaborateurs du SPEN. C'est pourquoi la GDR est un enjeu crucial pour ce service.

La culture organisationnelle du SPEN, fortement axée sur la sécurité, est promue à tous les niveaux de l'institution. Un livret d'accueil pour les collaborateur·trice·s met en évidence les valeurs du SPEN et les deux tiers environ du personnel sont assermentés.

Des retours d'expérience (RETEX) sont notamment réalisés après chaque événement ou chaque situation non maîtrisée, ce qui permet une amélioration continue. Concernant le risque sécuritaire, le SPEN est en perpétuelle évolution. Il existe une culture d'apprentissage permanent et le service doit constamment anticiper et s'adapter à l'émergence de nouveaux risques.

Objectifs et risques principaux

Des objectifs annuels sont définis pour le service, déclinés par entité et communiqués au sein du SPEN. Les objectifs opérationnels font l'objet d'un suivi dans les bilatérales entre le chef de service et les directeur·trice·s d'entités.

Selon le rapport sur la politique pénitentiaire de 2015, les objectifs stratégiques en matière de sécurité sont les suivants :

- Garantir une évaluation dynamique des risques au sens large ;
- Faire évoluer de manière continue le concept de sécurité permettant d'apporter une réponse efficiente aux nouveaux facteurs de risques (drones, détection de téléphones mobiles, etc.), à l'évolution des prises en charge ou encore au développement des infrastructures carcérales ;
- Poursuivre progressivement la mise en œuvre du plan de sécurisation des différents sites cantonaux dans la mesure des moyens qui seront alloués.

Les principaux risques identifiés par le SPEN sont la surpopulation carcérale, les infrastructures vieillissantes et non adaptées, ainsi que le taux d'encadrement insuffisant. Un rapport très complet sur la politique pénitentiaire a été publié en 2015, détaillant les défis rencontrés et les priorités stratégiques à mettre en place pour les gérer.

Ressources humaines

Gérer les risques du SPEN implique notamment de porter une attention particulière à la gestion des ressources humaines (RH) pour maintenir un taux d'encadrement suffisant. Pour cette raison, un processus de recrutement rigoureux a été mis en place et des évaluations périodiques sont effectuées pour examiner les compétences et les performances des employé·e·s, permettant ainsi d'identifier les besoins en formation et de remédier aux lacunes éventuelles. Les cahiers des charges sont mis à jour régulièrement lors des entretiens d'appréciation, réalisés au minimum tous les deux ans ou à chaque réorganisation. L'ancienneté est reconnue et valorisée.

La formation et la sensibilisation du personnel, en particulier en matière de GDR, jouent un rôle clé dans la culture de sécurité. Des programmes de formation réguliers sont dispensés pour améliorer la compréhension des risques spécifiques liés au travail pénitentiaire et des meilleures pratiques pour y faire face sont mises en œuvre. Des exercices de simulation d'urgence sont également organisés pour renforcer la préparation du personnel à des situations critiques. Le programme des formations continues est adapté en fonction des événements récents. Des capsules vidéo sont notamment utilisées pour permettre un accès en tout temps à certaines formations.

Le DRH du SPEN élabore une gestion prévisionnelle des emplois et des compétences (GPEC) actualisée chaque année, en accord avec la vision stratégique des RH. Il existe également une politique de formation avec des directives et un budget dédié. Le SPEN privilégie l'évolution et la promotion interne, offrant ainsi des opportunités variées.

Depuis 2016, le SPEN a mis en place un programme de santé au travail. Il a établi diverses directives dans ce domaine, traitant notamment du personnel soumis à des horaires irréguliers, du « case management »[20], des stages, de la supervision, ou encore des entretiens formels avec la hiérarchie. À partir de 2023, une nouvelle politique de santé au travail est mise en œuvre, incluant une personne dédiée et un partenariat externe pour fournir une assistance sociale aux collaborateur·trice·s en difficulté.

[20] Méthode d'accompagnement permettant notamment de gérer les questions complexes relevant de la santé et des assurances.

Outils de communication interne

Le SPEN a mis en place un système complet de GDR, incluant l'identification, l'évaluation, la planification d'actions correctives et le suivi. Des processus formels sont établis pour analyser les incidents, les accidents et les rapports d'activités afin de prévenir les risques futurs.

Divers moyens de communication internes sont utilisés, notamment la documentation quotidienne des risques liés aux personnes détenues et des mesures prises. Des tableaux de bord sont également développés pour faciliter la communication et la gestion proactive des risques.

Interactions à plusieurs niveaux

Le SPEN est membre de plusieurs commissions intercantonales et concordataires. Outre le cadre légal et le contrôle effectué sur la gestion du SPEN par les organes cantonaux ordinaires, différents acteurs exercent également une surveillance étroite sur les conditions de détention des personnes détenues : le Comité européen pour la prévention de la torture (CPT), la Commission nationale de prévention de la torture (CNPT), la Commission des visiteurs du grand conseil (CPVGC), ainsi que plusieurs organes supra cantonaux.

Le SPEN interagit aussi régulièrement avec d'autres services : p.ex. une séance de coordination de la chaîne pénale se tient trimestriellement avec la police cantonale, la police municipale de Lausanne, l'Ordre judiciaire vaudois (OJV), le Ministère Public et le Service de la population (SPOP), ce qui permet d'échanger des informations et de coordonner les différences instances pour gérer les risques.

Outils d'identification et d'analyse des risques

Des protocoles stricts sont mis en place pour identifier, mesurer et atténuer les risques liés aux personnes détenues, garantissant ainsi la sécurité. Il s'agit d'évaluer la dangerosité des personnes détenues pour estimer le risque de récidive ainsi qu'en regard de l'objectif de réinsertion qui fait également partie des missions du SPEN.

La gestion des personnes détenues est menée sur la base d'outils de GDR utilisés au quotidien par le personnel concerné. Il s'agit de modèles reconnus servant à évaluer les risques liés à chaque personne détenue, tels que la fiche de tri de l'Office d'exécution des peines (OEP), qui vise à permettre de classer rapidement, objectivement et uniformément tout nouveau dossier en fonction de la nature et du risque que présente la personne condamnée, ainsi que par l'intermédiaire des évaluations criminologiques qui approfondissent encore les facteurs de risque. Ces deux volets (tri et évaluation) seront intégrés dès 2025 au Processus latin d'exécution des sanctions orientée vers le risque et les ressources (PLESORR).

Les différents risques (risques d'évasion, risques de sécurité à l'intérieur de la prison, risques liés au travail, gestion du risque détenu, risque d'image du service, etc.) sont formellement identifiés et traités au travers des diverses procédures mises en place.

Malgré l'absence d'une approche formalisée pour la GDR à l'échelle de l'ensemble de l'ACV, la culture du SPEN, conjuguée à la mise en œuvre de processus et d'outils appropriés, assure de gérer en continu les multiples risques associés aux activités de ce service.

2.2.2. Directions générales

Les deux directions générales auditées n'ont pas encore de système de GDR formalisé. Les principaux constats résultant de l'audit sont exposés ci-après.

Direction générale de l'emploi et du marché du travail (DGEM)

Quatre directions rattachées à la DGEM

A compter du 1er juillet 2022, le Conseil d'État a décidé de transformer le Service de l'emploi en Direction générale de l'emploi et du marché du travail. Une démarche participative a été enclenchée, avec le soutien de l'Unité de Conseil et d'Appui en management et organisation (UCA), dans le but de reconfigurer l'organisation et de construire une vision commune pour l'ensemble de la DGEM. Les activités, précédemment gérées par cinq entités, ont été revues et regroupées en quatre directions distinctes dès le 1er janvier 2023 : Surveillance du marché du travail (DISMAT), Autorité cantonale de l'emploi (DIACE), Insertion professionnelle et placement (DIPP), à laquelle les ORP sont rattachés, et Caisse cantonale de chômage (CCh). La réorganisation n'a pas modifié les activités gérées par les entités rattachées à la DGEM.

Ces quatre directions fonctionnent selon des approches différenciées. Une gamme variée de prestations est délivrée aux employeurs et aux demandeurs d'emploi. La surveillance du marché du travail fait également partie des missions. Il est à noter que la plupart de ces activités sont régies par des règles fédérales. Chaque direction a construit son SCI selon la base légale qui régit sa mission et les exigences de la Confédération. La DGEM doit désormais mettre en place les instruments nécessaires pour forger une vision d'ensemble, englobant la GDR, de la totalité de ses activités.

Culture orientée vers les résultats

Déjà existante avant la création de la direction générale, une culture de performance et d'atteinte d'objectifs est bien ancrée au sein des quatre directions rattachées à la DGEM. Des objectifs quantitatifs sont définis à partir des différentes missions et déclinés jusqu'au niveau individuel. Qu'il existe ou non des mandats de prestations avec la Confédération, la DGEM fixe pour chacune de ses composantes des objectifs pour cadrer l'action, tels que le nombre annuel de visites en entreprises effectuées par les inspecteur·trice·s ou encore le nombre de dossiers quotidiens traités par les juristes.

L'examen des résultats comporte des contrôles réguliers d'indicateurs, des évaluations de performance et des rétroactions visant à assurer une adhésion des cadres et du personnel aux objectifs stratégiques. Chaque direction dispose de son reporting et des points de situation intermédiaires sont réalisés tout au long de l'année pour mesurer la progression vers l'atteinte des objectifs. Les cahiers des charges n'incluent toutefois pas d'éléments spécifiques à la GDR, ceux-ci sont sous-entendus dans les responsabilités.

Une veille attentive est maintenue sur les évolutions contextuelles pouvant influencer les activités, particulièrement les facteurs impactant les financements fédéraux. Dans cette optique, la DGEM s'appuie sur une variété de sources externes, notamment le Secrétariat d'Etat à l'économie (SECO), les statistiques sur le marché du travail et les prévisions économiques. Cette démarche proactive permet d'anticiper et de réagir aux changements, ce qui contribue à réduire les risques. Le financement de la Confédération est lié au nombre de demandeur·euse·s d'emploi et la baisse importante du chômage

ces dernières années a obligé la DGEM à s'adapter. Si le budget diminue, les effectifs sont réduits grâce aux départs naturels et aux éventuels non-renouvellements des personnes engagées en CDD.

Outils de gestion et de communication interne

La DGEM peut se baser sur des outils informatiques robustes pour faciliter ses activités, notamment ceux fournis par le SECO, tels que PLASTA (système d'information en matière de placement et de statistique du marché du travail) ou SIPAC (système informatisé pour le traitement et le paiement des prestations de l'assurance chômage). Ces outils permettent l'extraction de données cruciales pour le suivi et le contrôle des résultats, contribuant ainsi à la réalisation des objectifs fixés.

Par ailleurs, des plateformes intranet Wiki ont été créées dès 2015 par chaque direction et sont régulièrement alimentées par des responsables désigné·e·s. Elles permettent une communication interne de la DG et également au sein des différentes directions. Les Wikis recensent tous les processus de travail documentés, les directives SECO, ainsi que les modalités de travail et d'autres documents utiles. Grâce à ces plateformes, une communication interne fluide ainsi que la recherche par mots-clés sont possibles.

Interactions intercantonales

Tous les cantons sont membres de l'AOST (Association des offices suisses du travail) qui anime des groupes thématiques (mesures du marché du travail (MMT), ORP, questions juridiques, directeur·trice·s) et des groupes régionaux. L'AOST a aussi pour but de défendre les intérêts cantonaux auprès du SECO (toutes les directives du SECO sont transmises via l'AOST pour consultation), d'animer des groupes de travail avec le SECO et de créer des formations. Elle n'émet toutefois pas de règles en matière de GDR.

En participant à des groupes intercantonaux, la DGEM récolte non seulement des informations, p. ex. à propos des modifications législatives, mais elle peut aussi mieux anticiper — voire influencer — les changements.

Certifications et contrôles fédéraux

La Caisse cantonale de chômage (CCh) se distingue par sa certification *ISO 9001:2015* depuis plus de dix ans (renouvellement de la certification prévu en 2023), témoignant d'une maturité avancée en matière de GDR. Cette certification intègre des éléments liés à la GDR et nécessite une démarche proactive pour identifier et atténuer les menaces. Dans ce cadre, la CCh a établi une *cartographie de ses risques*, évalué leur probabilité et criticité, et décrit des mesures prévues. Elle a aussi mis en place un processus d'amélioration qui permet aux collaborateur·trice·s d'alimenter le système (EINSTEIN) et les points soulevés sont traités en comité de direction. La DIACE et la LMMT[21] avaient également établi une *cartographie des risques* pour leurs activités en 2017-18. Ce travail avait été mené à terme, mais pas tenu à jour.

Globalement, la DGEM doit davantage rendre compte à la Confédération qu'au CE. Les mandats fédéraux imposent une exécution très normée. Des contrôles fédéraux réguliers ainsi que des audits aléatoires, pouvant remonter jusqu'à trois ans en arrière, contribuent à une gestion proactive des risques et à une amélioration continue. Notamment, l'organe de révision du SECO effectue des

[21] Les mesures du marché du travail (LMMT) ont été fusionnées avec le service de coordination des offices régionaux de placement (ORP) dans la nouvelle organisation pour former la DIPP.

contrôles quantitatifs et qualitatifs des activités ainsi que des audits d'ORP et d'agences de la CCh. Cela peut donner lieu à des demandes de mesures correctives, avec un délai de traitement défini. Ces contrôles permettent aussi de vérifier la bonne adhésion du personnel aux procédures.

Une vision morcelée de la GDR de la DGEM

Malgré les éléments positifs relevés ci-dessus, à ce jour, il n'existe pas de politique interne formelle spécifique à la GDR et des pratiques différentes sont constatées entre les quatre directions rattachées à la DGEM. Il en résulte des degrés de maturité variables dans la GDR.

Il n'existe pas de *cartographie des risques* de l'ensemble de la DGEM ni de liste formalisée, mais uniquement une analyse réalisée pour le SCI financier, ainsi que des cartographies sectorielles réalisées au sein de certaines directions, en particulier celle de la CCh effectuée dans le cadre de sa certification ISO. Il n'y a donc pas de vision globale à jour et documentée du portefeuille des risques au niveau de la DGEM, avec évaluation de la criticité de ces risques et identification des modalités de traitement. Un système de GDR n'étant pas encore instauré, celui-ci ne peut pas être mis à jour et ne fait pas l'objet d'un processus d'amélioration continue. En instaurant ceci, la direction générale disposerait d'un tableau de bord permettant d'avoir une vision d'ensemble des risques liés aux activités des quatre directions et de gérer les risques transversaux de manière performante.

Direction générale de l'enseignement postobligatoire (DGEP)

14 gymnases et 13 établissements de formation professionnelle rattachés à la DGEP

Alors que les gymnases et les écoles professionnelles sont rattachés fonctionnellement à la direction générale, les directeur·trice·s d'établissement sont engagé·e·s par le CE. Une organisation-cible est proposée aux directions d'établissements et différentes démarches en cours ont pour objectif l'harmonisation des processus. Les gymnases et les écoles professionnelles conservent toutefois une certaine autonomie, ce qui conduit à des pratiques différenciées. Notamment la conduite pédagogique relève de la responsabilité des établissements, dans le cadre de la grille horaire définie par la Conférence des directrices et directeurs cantonaux de l'instruction publique (CDIP). Les gymnases et les écoles professionnelles ne sont pas soumis aux mêmes bases légales : la formation professionnelle regroupe 175 métiers différents régis par le droit fédéral, alors que la formation gymnasiale fait l'objet d'un plan d'études, avec une liberté pédagogique inscrite dans la loi.

Ressources humaines

L'autorité d'engagement des enseignant·e·s n'est pas la direction des établissements, mais la DGEP. Il n'y a en revanche pas de suivi centralisé des formations continues et l'évaluation des enseignant·e·s n'est pas pratiquée, ce qui augmente le niveau de risque. Au sein de la direction générale et des unités administratives qui lui sont rattachées (appelés « la centrale » par la DGEP), des entretiens d'appréciation sont en revanche réalisés pour chaque collaborateur·trice au minimum tous les deux ans.

Outils de communication interne

Des informations sont disponibles via un Wiki pour les collaborateur·trice·s de la centrale et les directions d'établissements. A ce jour, le corps enseignant n'a pas accès à l'espace documentaire géré par la centrale, ce qui ne permet pas une communication ascendante et descendante fluide.

Démarches qualité en cours

La DGEP a mis en place un cadre de certification, laissant la liberté aux établissements de choisir la norme qu'ils souhaitent appliquer parmi trois standards applicables aux établissements de formation.

Dans les écoles professionnelles, les démarches de certification sont menées par des responsables qualité, identifiés dans chaque établissement (enseignant·e, doyen·ne ou administrateur·trice). La plupart de ces établissements ont obtenu une certification : huit sont certifiés QSC[22] ; un est certifié ISO9001 et eduQua[23] ; deux sont certifiés ISO21001 et un est en cours d'obtention de cette certification ; la certification d'une école est actuellement en attente en raison d'un changement de direction à venir.

A ce jour, aucun gymnase n'a lancé de démarche de certification. Une certification des gymnases était prévue et trois établissements pilotes avaient été désignés, avec la définition d'objectifs, de personnes responsables et d'un planning. La DGEP indique qu'une décision politique de geler la démarche a été prise, en raison de sa faible acceptabilité sur le terrain. Avec le prochain passage du gymnase en quatre ans, des exigences fédérales seront fixées en matière de comparabilité des formations cantonales qui nécessiteront vraisemblablement que les écoles se dotent d'un dispositif de développement et d'assurance-qualité[24].

Au niveau de la centrale, un projet nommé « Fondations » vise à formaliser les processus, ce qui permettra l'identification des risques. De plus, la certification ISO de la centrale est en cours. La DGEP est consciente de devoir améliorer et poursuivre les démarches entamées, mais elle souhaite d'abord mettre en place des tableaux de bord financiers et informatiser tous les processus avant d'instaurer une GDR formalisée.

Gestion de risques spécifiques liés aux bâtiments

Entre 2019 et 2022, la DGEP a mandaté des cabinets spécialisés pour identifier les risques liés aux bâtiments. A ce jour, 15 établissements (sur 26) du secondaire II ont été analysés. Des mesures correctrices ont été définies et sont suivies. Concernant la sécurité des bâtiments et la santé au travail, la DGEP indique que ces risques seront pris en charge conjointement avec la DGIP et la DGRH.

L'un des principaux risques identifiés par la DGEP est celui de manquer de capacité d'accueil dans les bâtiments scolaires du secondaire II, en particulier dans les gymnases. Afin d'éviter ce risque, la DGEP a mis en place un système de prévision des classes à 10 ans permettant de planifier la construction et l'agrandissement des bâtiments avec la DGIP. Néanmoins, certains projets ont connu des reports

[22] *Quality School Certificate*, en français Certificat suisse de qualité pour les écoles d'enseignement général et professionnel. Il s'agit d'un référentiel élaboré spécifiquement en vue de la mise en place dans les écoles d'un système de « gestion qualité ». Le but est de répondre aux exigences légales fédérales et cantonales quant au développement de la qualité dans les écoles professionnelles.
(source : https://www.procert.ch/fr/faq/qsc2016-53.html)

[23] Label qualité conçu et développé spécifiquement pour les prestataires de formations continues en Suisse. eduQua a été créé en 2000, à l'initiative du Secrétariat d'État à l'économie (Seco), de l'ancien Office fédéral de la formation professionnelle et de la technologie (OFFT), de la Conférence des Offices suisses alémaniques de la formation professionnelle (DBK) et de la Fédération Suisse pour la formation continue (FSEA) (source : https://alice.ch/app/uploads/2022/11/eduqua-2021-norm-f.pdf)

[24] Voir art. 28 et 29 de l'ordonnance sur la reconnaissance des certificats de maturité (ORM), version provisoire du 23.06.2023

successifs de plusieurs années, en raison de facteurs externes à la DGEP. Toutefois, des solutions de location et d'aménagement de surfaces supplémentaires ont pu être réalisées dans les temps, bien que dans l'urgence.

Gestion de risques liés aux projets informatiques
Une politique de sécurité a été adoptée, définissant les objectifs pour la sécurité de l'ensemble des données, des systèmes d'information, des applications et réseaux détenus et gérés par la DGEP. Il existe une bonne collaboration avec la DGNSI pour le suivi des risques des projets informatiques. Des comités de pilotage sont en place pour suivre régulièrement ces projets, analyser leurs risques et prendre les mesures nécessaires.

Pas de vision globale de la GDR au niveau de la DGEP
A ce jour, il n'existe pas de politique interne formelle sur la GDR. Compte tenu de l'autonomie des établissements, la centrale a peu de visibilité sur leurs activités et un pouvoir d'action limité.

La DGEP n'a pas établi de liste ni de *cartographie des risques*, hormis pour le SCI financier. Elle n'a donc pas évalué la criticité des risques et ne les a pas priorisés. Il n'y a pas non plus de documentation sur les mesures prévues pour chacun des risques. La DGEP analyse uniquement les risques liés à des projets, ou spécifiques à un problème donné (p.ex. bâtiments). Etant donné l'absence actuelle d'un système de GDR, celui-ci ne peut pas être mis à jour et ne fait pas l'objet d'un processus d'amélioration continue.

2.2.3. Entités transversales

La Chancellerie d'Etat (CHA) et le SG-DITS ont des résultats similaires. A l'heure actuelle, la mission de ces entités ne comprend pas formellement d'éléments relatifs à la GDR, ni à l'interne de chacune d'elles, ni pour assurer la cohérence entre les départements ou entre les services.

Secrétariat général du Département des institutions, du territoire et du sport (SG-DITS)

Position centrale du SG
Le SG-DITS occupe une position centrale, qui lui donne accès à une vaste gamme d'informations relatives aux activités de l'ACV. Le SG maintient des contacts réguliers non seulement avec la cheffe du département, qui assume également la présidence du CE pour la présente législature, mais également avec l'ensemble des entités du département. Grâce à sa participation à diverses séances ainsi qu'à travers la communication quotidienne avec les services, le SG-DITS contribue à la préparation et au suivi des décisions prises par le CE. Lors des sessions hebdomadaires de débriefing qui suivent les séances du CE, une attention particulière est accordée à l'examen des risques, qu'ils soient de nature politique, opérationnelle ou de communication. Le SG-DITS identifie et évalue ces risques de manière individuelle, mais cette approche ne fait pas l'objet d'un processus formalisé de GDR.

Une veille sur les affaires fédérales et intercantonales est exercée par l'Office des affaires extérieures (OAE), qui est rattaché au SG-DITS. Cette démarche offre une source substantielle d'informations, aux niveaux fédéral et intercantonal, concernant l'évolution contextuelle et l'émergence de nouveaux risques. En outre, un suivi des affaires communales est assuré en collaboration avec les préfectures. Enfin, des échanges hebdomadaires au sein du collège des secrétaires généraux de départements

(CSG) permettent la mise en commun d'informations entre les différents départements, notamment sur les projets à caractère transversal. Les objets portés par des services transversaux sont présentés au CSG qui examine les préavis et joue un rôle de détection des risques liés à ces projets.

Outils de communication
Le délégué départemental à la communication rattaché au SG-DITS gère le plan de la communication et coordonne les actions proactives du département. Ces tâches nécessitent une évaluation préalable des risques et impliquent une collaboration constante avec les responsables de la communication des services rattachés au DITS, le Bureau d'information et de communication (BIC), et, au besoin, des autres départements.

Concernant la communication réactive, une note interne au DITS, validée par la cheffe de département, prodigue des conseils en matière de relation avec les médias. Cette note précise par ailleurs qui est habilité à communiquer avec les journalistes et, par-là, les niveaux de validation des réponses qui seront données.

Ressources humaines
Les cahiers des charges qui définissent les rôles et responsabilités des collaborateur·trice·s du SG ne mettent pas en évidence les aspects liés à la GDR, bien que ces éléments soient implicitement inclus dans les attributions de chacun·e.

Au niveau du département, une politique globale de gestion des RH n'a pas encore été instaurée. La responsable RH départementale joue un rôle distinct des responsables RH (RRH) de services impliquant des missions complémentaires. Cela inclut le conseil et le soutien à la cheffe du département pour toute question relative aux RH, le conseil aux chef·fe·s de service et aux RRH de service, l'élaboration et la consolidation de rapports RH, ainsi que l'animation du réseau des partenaires RH du département. Par ailleurs, elle prend en charge des tâches RH pour les services qui ne disposent pas de personnel dédié.

Certaines procédures et listes de contrôle sont établies par divers·e·s RRH sur des supports différents. Cette absence d'harmonie et le manque d'outils transversaux peuvent compliquer la centralisation et la consolidation des informations.

La question de la relève revêt une importance particulière, compte tenu du nombre élevé de départs à la retraite prévus parmi les cadres dans les années à venir. Il est à noter que le SG se montre attentif aux besoins détectés et encourage les demandes de formation.

Finances
A l'instar de la communication et des RH, la gestion financière est également une fonction transversale, exercée par la responsable financière départementale engagée au sein du SG-DITS. Cela englobe d'une part le suivi budgétaire, la comptabilité ainsi que la clôture des comptes pour le SG. D'autre part, la responsable financière départementale prend en charge les aspects liés à l'élaboration du budget et au bouclement des comptes pour le département dans son ensemble.

Le SG doit s'assurer que les directives du SAGEFI sont connues et respectées et que chaque service remonte bien l'information. La responsable départementale diffuse des instructions, puis organise une réunion avec les responsables des services pour garantir une compréhension précise de ces instructions et s'assurer que les délais prescrits sont tenus. De plus, elle a formé chaque responsable

comptable du DITS à l'utilisation du « Business warehouse », un programme qui permet un suivi financier des projets et des comparaisons entre les budgets.

Les contrôles relatifs aux états financiers sont cadrés par le SCI qui a été certifié en 2011.

Absence de GDR formalisée au sein du SG-DITS

Actuellement, il n'existe pas de processus formalisé permettant d'identifier et d'évaluer les risques propres aux activités du SG-DITS. Seuls les risques liés aux états financiers ont été analysés dans le cadre du SCI, avec des enjeux faibles pour le SG qui est une petite unité d'environ 20 personnes. Les changements contextuels majeurs pouvant influencer les risques sont traités au cas par cas, sans qu'une évaluation périodique soit réalisée pour documenter ces évolutions dans un système formalisé et pour intégrer les risques émergents. Toutefois, comme pour tous les services de l'ACV, des plans de gestion de crise et de continuité ont été récemment élaborés en réponse à la pandémie et au risque de pénurie énergétique.

La prise de décision et la gestion des activités au sein du SG-DITS reposent principalement sur des séances bilatérales entre le chef de service et les responsables d'unités (RH, finances, communication). Bien que les procès-verbaux de ces séances ainsi que divers documents permettent de suivre les affaires en cours, il n'existe pas de documentation spécifiquement consacrée à la GDR. La plupart des informations traitées par le SG-DITS sont gérées au moyen de fichiers Word ou Excel, tels que tableaux de suivi des projets DITS et de planification de leur passage au CE, agenda permanent RH listant les différentes tâches à effectuer au cours de l'année, planning des communications du DITS, etc.

Les objets parlementaires sont quant à eux traités dans SIEL, ce qui assure la traçabilité des informations et permet de suivre les échéances et les tâches (p.ex. transférer des courriers entre départements). Grâce à cette plateforme, les informations peuvent aisément descendre vers les services, et vice-versa.

Pas de coordination de la GDR pour le département

Les principales fonctions du SG sont[25] :

- l'appui à la cheffe de département comme membre du collège gouvernemental ;
- le soutien à la cheffe de département dans la direction du département ;
- l'appui aux services en matière de finances, ressources humaines, conseil juridique, communication et planification stratégique ;
- la représentation des intérêts du département vis-à-vis des services transversaux, en particulier pour les questions de finances, ressources humaines et informatiques ;
- la représentation du département auprès des pouvoirs législatifs et judiciaires du canton, ainsi que des autres institutions de l'administration cantonale, intercantonale et fédérale.

Le SG est donc notamment chargé de soutenir les services du département dans les différents domaines transversaux. Ses objectifs sont définis annuellement, en cohérence avec le programme de législature, au cours d'une séance rassemblant l'état-major, les responsables d'unité du SG, les adjoint·e·s au SG et les chef·fe·s de service. Cette démarche fournit un socle sur lequel s'appuyer pour

[25] Source : https://www.vd.ch/toutes-les-autorites/departements/departement-des-institutions-du-territoire-et-du-sport-dits/secretariat-general-du-departement-des-institutions-du-territoire-et-du-sport-sg-dits

la réflexion et la documentation des risques, ainsi que pour la formulation de mesures préventives et de stratégies de gestion.

Le rôle actuel du SG ne comprend toutefois pas la supervision de la GDR des services ni l'identification et l'agrégation des risques majeurs du département. Par conséquent, le SG ne contribue pas à l'élaboration d'une vision globale à jour et documentée du portefeuille des risques des entités du DITS qui pourrait être transmise à la cheffe de département.

Chancellerie d'Etat

Position centrale de la Chancellerie

Les missions et activités de la Chancellerie d'Etat (CHA) sont principalement encadrées par la loi sur l'organisation du Conseil d'Etat (LOCE). Les autres entités qui lui sont rattachées (BIC, Bureau cantonal de médiation administrative (BCMA), Archives cantonales et Autorité de protection des données et de droit à l'information (PPDI)) disposent elles aussi de bases légales précises détaillant leurs prestations. Occupant une position centrale, la CHA est notamment responsable de coordonner et de vérifier la bonne application des décisions du CE conformément à l'art. 37 de la LOCE et l'art. 12 al. 2 du Règlement sur les départements de l'administration (RdéA).

La GDR au sein de la CHA est principalement axée sur la sécurité et la précision de la retranscription des décisions gouvernementales, ainsi que sur leur diffusion efficace. Un suivi est ensuite effectué pour s'assurer de la mise en œuvre effective de ces décisions. Les réunions hebdomadaires de débriefing des séances du CE offrent l'opportunité de passer en revue les risques, en particulier les risques opérationnels et de communication. Par ailleurs, le Chancelier préside les réunions hebdomadaires du CSG, au cours desquelles ont lieu des échanges sur les dossiers en cours, ce qui permet une coordination entre les différents acteurs.

SIEL, principal outil de gestion documentaire

L'application SIEL, utilisée par tous les services de l'ACV, constitue un outil majeur pour le suivi des sujets traités par le CE et le GC, et vise une communication interne efficace, ainsi qu'un suivi et un archivage adéquats. Parallèlement, SIEL a joué un rôle déterminant dans l'harmonisation des pratiques au sein de l'administration. Après les séances du CE et du GC, il permet de vérifier les statuts de décision pour chaque sujet, d'effectuer un suivi et de fixer définitivement le texte des décisions gouvernementales.

Bien que SIEL soit l'outil informatique principal employé par la CHA, il n'est pas spécifiquement destiné à la communication relative à la GDR (laquelle n'est pas formalisée en tant que telle). La CHA estime qu'il serait toutefois envisageable d'explorer davantage ses capacités, notamment pour créer des tableaux de bord plus élaborés facilitant la GDR.

Notes et propositions au Conseil d'Etat

La LOCE prévoit une obligation d'information des départements envers le collège exécutif. A cette fin, les chef·fe·s de département rédigent des « Notes au CE » qui intègrent systématiquement une section consacrée aux « Enjeux/Risques politiques/Incidences », dont l'objectif est d'analyser de manière ciblée certains risques spécifiques.

Les propositions au Conseil d'Etat (PCE) constituent l'instrument formel à utiliser par les différentes entités au sein de l'ACV pour présenter au CE des idées, des initiatives ou des actions concrètes en vue

de leur évaluation, de leur débat, de leur validation et de leur mise en œuvre. L'analyse et l'évaluation des risques associés à la proposition, qui représentent un élément clé des PCE, englobent généralement une description détaillée des risques, incluant en particulier les risques financiers, mais aussi les risques politiques, juridiques, environnementaux, etc. Lorsqu'ils sont impliqués dans un projet, les services transversaux doivent également être sollicités pour délivrer leur préavis en amont des décisions. Le rôle de la CHA réside dans la vérification de l'exhaustivité des PCE, y compris la présence des avis préalables requis. Ainsi, la PCE joue un rôle essentiel en tant qu'outil de synthèse et de liste de contrôle. L'objectif global de ce processus est d'identifier et de réduire les risques associés aux projets présentés pour décision au Conseil d'État.

Suivi du programme de législature

Pour élaborer le programme de législature, les membres du CE disposent d'une analyse interne réalisée par chaque service, sous la supervision de leurs départements respectifs. Cette analyse englobe plusieurs aspects cruciaux, notamment l'évolution générale de l'environnement et des principaux enjeux auxquels chaque service est confronté, les contraintes, les risques et les opportunités spécifiques à leur domaine d'activité, ainsi que les impacts majeurs sur leurs missions.

Le suivi du programme de législature est placé sous la direction de la CHA. Les résultats intermédiaires sont rendus publics dans le rapport annuel du CE qui comprend un chapitre dédié à l'état d'avancement des mesures du programme de législature. Des bilans sont également réalisés à mi-législature et en fin de législature. La rédaction de base de ces bilans est assurée par les départements qui en sont les responsables, tandis que la CHA coordonne le tout et en effectue un suivi.

La CHA veille à la mise en œuvre cohérente de ce programme, qui englobe non seulement les objectifs gouvernementaux prioritaires, mais aussi l'ensemble des activités régulières des services. Cette démarche trouve sa justification notamment dans la LOCE (art. 37).

Absence de GDR formalisée au sein de la Chancellerie

Au début de l'année 2023, le CCF a certifié le SCI financier de la CHA, ce qui a nécessité l'identification des processus financiers, la *cartographie des risques* qui y sont inhérents, ainsi que la description des contrôles en place pour en atténuer les impacts. Par ailleurs, comme les autres services de l'ACV, en raison des événements survenus ces dernières années, la CHA a développé des plans de continuité et de gestion de crise. Cependant, en l'absence d'une politique formelle sur la GDR définie au niveau cantonal, les autres types de risques n'ont pas été identifiés ni analysés, et les modalités de traitement correspondantes ne sont pas documentées.

Les conclusions rejoignent donc celles exposées précédemment pour le SG-DITS. La Cour constate l'absence d'une GDR formalisée pour la CHA et les entités qui lui sont rattachées.

Pas de coordination de la GDR pour les différents départements

La présidence quinquennale renforce la responsabilité de la CHA dans son rôle d'appui à la présidence et de suivi des affaires auprès des départements. Le rôle actuel de la CHA vis-à-vis des départements ne comprend toutefois pas la supervision et la centralisation de la GDR dans un système formalisé. Il n'existe pas encore de procédure établie pour l'identification et la remontée au CE des risques majeurs de l'ACV.

3. Mise en place d'une GDR intégrée

3.1. Définir une gestion intégrée des risques pour l'ACV

Comme précédemment indiqué, il n'existe pas à ce jour de stratégie définissant la GDR voulue pour l'ACV. Les résultats présentés au chapitre 2.2. illustrent l'approche opérationnelle et non homogène mise en œuvre actuellement par les services qui en découle. Afin de remédier à ces pratiques non harmonisées et peu, voire pas, formalisées pour certains services, il est nécessaire que le CE définisse une vision globale et donne une impulsion à l'instauration d'une véritable *gestion intégrée des risques* pour l'ensemble de l'ACV.

C'est la raison pour laquelle toutes les recommandations découlant des constatations figurant au chapitre 2 sont adressées au Conseil d'Etat. Ces recommandations sont organisées en cascade, allant de la définition de la GDR souhaitée jusqu'à sa mise en place par étapes et son suivi.

3.1.1. Définir une politique cantonale homogène

Une stratégie à définir

Une stratégie en matière de risques est essentielle pour toute organisation, car elle établit les principes fondamentaux nécessaires à une GDR efficace et proactive. Elle doit définir clairement les objectifs de la GDR, qui englobent notamment la préservation des ressources, la protection des biens et des personnes, l'amélioration de la prise de décision et la garantie de la continuité des activités critiques. Cela implique de trouver un équilibre entre les opportunités et les menaces, tout en déterminant les limites à ne pas dépasser en matière de prise de risque (*tolérance au risque*) et en identifiant les mesures possibles pour les maîtriser.

Dans certains cas, des risques liés à l'exécution des tâches de l'administration publique ne peuvent être totalement évités. C'est pourquoi il est nécessaire de prendre des risques contrôlés pour atteindre les objectifs opérationnels de l'Etat ainsi que ceux énoncés dans le programme de législature, tout en veillant à une utilisation économe des ressources. Une approche réfléchie et proactive en matière de GDR est donc cruciale pour assurer l'accomplissement de la mission de l'Etat auprès des citoyen·ne·s, tout en minimisant les impacts négatifs liés à la prise de risque.

De manière générale, la stratégie doit indiquer comment la GDR est mise en œuvre. Dans de grandes organisations telles que l'ACV, il s'avère judicieux d'établir une stratégie globale, souvent appelée « politique de *gestion des risques* », qui est ensuite déclinée dans les départements et services. Pour assurer un déploiement cohérent, cela implique que cette démarche soit initiée par le CE.

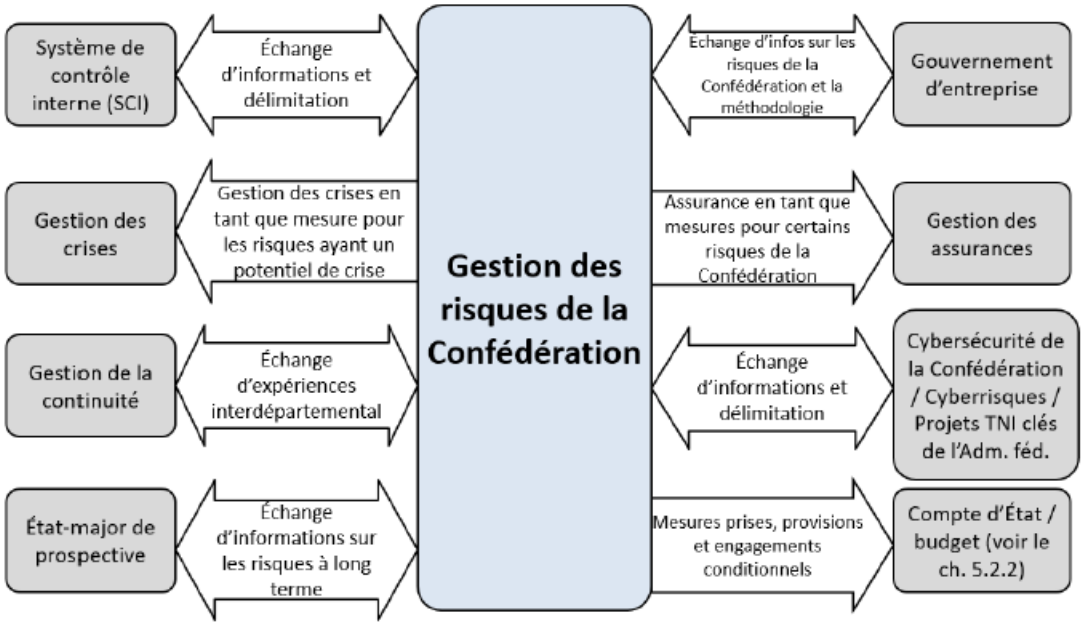
Une fois la stratégie de GDR définie au niveau le plus élevé de l'ACV, il incombe à chaque département, puis chaque direction générale ou service, de la mettre en pratique dans son domaine. Cela conduit à fixer des objectifs spécifiques en matière de GDR et à déterminer comment cette dernière sera concrètement appliquée.

Cette stratégie doit être largement diffusée au sein de l'ACV et servir de référence pour les décisions liées à la GDR, contribuant à créer une culture du risque partagée. Ainsi, la politique de GDR permet également de s'assurer que l'ensemble du personnel partage la même *appétence au risque*.

Des interfaces avec d'autres activités

Le SCI, la gestion des urgences et des crises, ainsi que les plans de continuité sont des outils complémentaires à la GDR. Il doit donc exister des interfaces et des flux d'informations entre les différents projets et fonctions pour éviter les redondances et gaspillages.

An niveau de la Confédération, ces interfaces peuvent être illustrées comme suit :



Source : Manuel de gestion des risques de la Confédération

Les interfaces entre la GDR et les principaux domaines concernés, qui visent à assurer une approche globale et intégrée de la sécurité et de la continuité des activités, sont les suivantes :

1. **Système de contrôle interne (SCI) :** Alors que la GDR se caractérise par sa large portée, le SCI se concentre spécifiquement sur les risques ayant un impact sur les états financiers et sur la mise en place de mesures de contrôle visant à les atténuer. En conséquence, le SCI fait partie intégrante de la gestion globale des risques. Pour optimiser le travail et assurer une gestion cohérente, les risques pertinents déjà identifiés dans le SCI financier doivent être repris dans l'analyse de GDR et complétés de tous les autres risques (stratégiques et opérationnels). Il peut être aussi nécessaire d'adapter le SCI pour intégrer des risques supplémentaires identifiés dans le cadre de la GDR.
2. **Gestion des urgences et des crises :** Cette gestion est étroitement interconnectée avec la GDR, car cette dernière permet d'anticiper les risques et de se préparer aux mesures à prendre en cas d'incidents majeurs. La GDR englobe la détection précoce des risques qui vise une mise en place rapide de mesures efficaces pour faire face aux situations d'urgence ou de crises lorsqu'elles surviennent. Dans une démarche d'amélioration continue, elle intègre également les enseignements tirés des crises passées pour renforcer la préparation aux risques futurs.
3. **Plans de continuité :** Un système intégré de GDR comprend la gestion de la continuité (Business Continuity Management, BCM). Alors que la GDR évalue préalablement les dangers pouvant affecter l'exécution des tâches et l'atteinte des objectifs, la BCM se concentre sur la gestion d'un événement en cherchant à atténuer l'impact sur les prestations et processus

opérationnels essentiels pour permettre à l'organisation de continuer à fonctionner a minima, même en situation de crise. Dans le cadre de la GDR, la BCM est donc considérée comme une mesure qui agit sur les conséquences des risques identifiés. Un exemple récent de plan de continuité est celui développé en 2022 par les services de l'ACV pour faire face au risque de pénurie énergétique (mention au chapitre 2.1.2).

Une volonté du CE de renforcer la résilience aux risques

Le programme de législature 2022-2027 du Conseil d'Etat prévoit déjà de « renforcer la transversalité de l'action publique et la résilience du Canton, notamment en matière de prévention des risques et de gestion de crise » (mesure 3.18). Pour ce faire, le CE a défini l'action suivante : « Renforcer la résilience du Canton face aux risques notamment en renforçant la culture de gestion de crise au sein de l'administration cantonale, en soutenant les communes dans ce domaine et en analysant les capacités cantonales à faire face aux risques et aux crises dans le cadre d'une approche globale des dangers. » L'adoption d'une politique de GDR, à l'instar de celle établie par la Confédération en 2004[26], s'intègre parfaitement dans cet objectif et constitue le fondement d'un système de *gestion intégrée des risques*, raison pour laquelle la recommandation suivante est adressée au CE :

Définir une politique cantonale homogène	
Recommandation n° 1	**au Conseil d'Etat**
Elaborer une stratégie formelle en matière de *gestion des risques* visant une approche commune pour l'Etat de Vaud qui inclut la gestion de l'ensemble des risques qui peuvent influer sur la réalisation des mesures figurant dans le programme de législature et des objectifs opérationnels au sein des différents services de l'Etat.	

3.1.2. Elaborer des directives

Des principes et méthodes à uniformiser

Des politiques internes, telles que la politique relative à la sécurité informatique ou la politique de gestion des dangers naturels évoquées au chapitre 2.1.2, abordent certains risques spécifiques. Toutefois, pour instaurer à l'ACV un système de *gestion intégrée des risques* véritablement efficace et cohérent, il est essentiel de développer des directives qui définissent les normes minimales requises. Ces directives jouent un rôle central en garantissant que tous les niveaux de l'ACV sont sensibilisés aux risques et contribuent ainsi à renforcer la culture de la gestion des risques.

Des directives concrétisent la stratégie en fournissant des règles claires et permettent ainsi d'avoir une vision globale de tous les risques et de leur gestion. Elles doivent préciser le périmètre d'application, en identifiant les services administratifs concernés, les normes, les processus inclus, les principes et les méthodes qui doivent être appliqués par les différent·e·s intervenant·e·s, ainsi que les types de risques à prendre en compte.

[26] Politique de gestion des risques, Bases pour la gestion des risques au sein de la Confédération, Département fédéral des finances, décembre 2004

Il est ainsi nécessaire d'établir les attentes minimales en matière de GDR au sein des services de l'administration, notamment en définissant des règles pour :

- l'identification et la classification des risques ;
- l'analyse et l'évaluation des risques ;
- le traitement des risques ;
- la communication et le reporting (voir chapitre 3.2.3.) ;
- le suivi, l'évaluation et l'amélioration continue (voir chapitre 3.3.).

Cette approche permet de fournir un cadre général et d'éviter que chaque direction générale ou service consacre du temps à choisir un modèle de référence et à définir une méthodologie. Cela favorise une gestion homogène et intégrée des risques à tous les niveaux de l'ACV. En harmonisant les pratiques, les différents risques sont évalués de manière comparable, ce qui facilite également leur consolidation et permet de remonter les informations au niveau approprié.

Les différentes phases de processus de GDR sont décrites ci-après :

L'identification et la classification des risques

La première étape cruciale du processus de GDR consiste à appliquer une approche méthodique pour identifier et classifier les risques. Ces derniers sont définis comme les « effets de l'incertitude sur l'atteinte des objectifs ». Pour les identifier, il est donc essentiel de se baser sur les objectifs et les tâches des directions générales et services, découlant notamment des bases légales, ainsi que sur les objectifs définis dans le programme de législature.

Diverses méthodes peuvent être utilisées pour valoriser la connaissance du terrain, par exemple des ateliers ou des entretiens avec les membres de la direction et/ou du personnel spécialisé dans des domaines spécifiques (détenteurs du savoir).

Il est possible d'établir des catégories pour classifier et regrouper les risques comme l'a fait p.ex. la Confédération en définissant six catégories : financiers et économiques/juridiques et conformité/matériels, techniques et liés aux éléments naturels/liés aux personnes et à l'organisation/technologiques et biologiques/sociaux et politiques.

Malgré toute la rigueur apportée à l'identification, il est important de reconnaître que des *risques résiduels* non identifiables et non gérables subsisteront toujours. En effet, certains risques peuvent échapper à la détection en raison d'une vision limitée ou d'un manque d'anticipation de l'organisation, ou encore de l'émergence de phénomènes imprévisibles. Le but est donc d'obtenir une liste aussi exhaustive que possible des risques pouvant potentiellement affecter négativement l'exécution des tâches et la réalisation des objectifs de l'ACV.

L'analyse et l'évaluation des risques

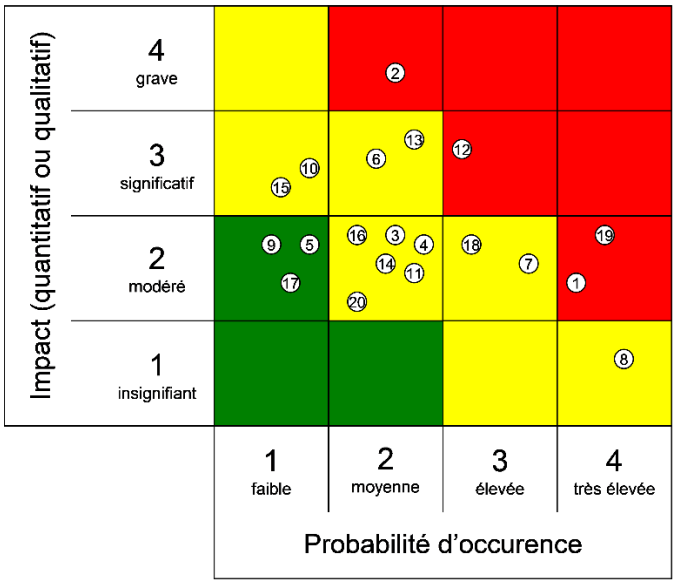
Chaque risque identifié doit faire l'objet d'une analyse afin de déterminer ses causes et conséquences potentielles. De plus, une réflexion sur les éventuelles interactions avec d'autres risques est menée pour obtenir une vision globale et cohérente des scénarios possibles.

Il est également très important de désigner un·e « *propriétaire* » pour chaque risque identifié, au niveau pertinent, le plus bas possible dans la hiérarchie, de manière à associer un maximum de

personnes à cette mise en place de la GDR. En intégrant la surveillance et le traitement des risques dans les cahiers des charges des personnes concernées, on peut ainsi s'assurer de la bonne qualité de la GDR et éviter de créer une structure administrative parallèle.

La probabilité d'occurrence du risque et la sévérité de ses conséquences sont ensuite évaluées. Cette appréciation ne se limite pas seulement à des critères financiers, mais prend également en compte d'autres effets tels que les atteintes à la réputation ou les impacts sur les processus opérationnels, ainsi que les dommages corporels et environnementaux, afin de mieux cerner l'ampleur réelle du risque. Les mesures d'atténuation déjà mises en œuvre, de même que celles envisagées doivent être documentées pour évaluer le *risque résiduel*. Les critères d'évaluation de la probabilité et de l'impact doivent être définis pour assurer une application homogène au sein de l'ACV.

A ce stade, une analyse de scénarios peut être effectuée, pour illustrer de manière concrète l'impact potentiel d'un risque. Par exemple, en évaluant les dommages selon trois options différentes, il est possible de mieux comprendre l'ampleur des conséquences envisageables et de prévoir des mesures adaptées pour faire face aux différents scénarios.



Source : Cour des comptes 2013

Le résultat de cette phase est généralement représenté sous forme de *cartographie* (aussi appelée matrice) *des risques* telle que celle figurant ci-dessus. Idéalement, l'évaluation doit porter à la fois sur les *risques inhérents* et sur les *risques résiduels*.

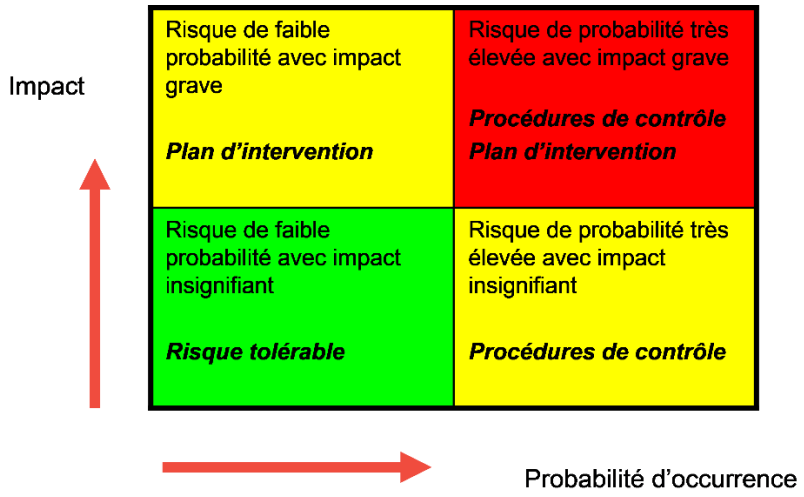
Le traitement des risques

Les mesures de traitement sont cruciales pour faire face aux risques identifiés. Selon l'importance du risque et la *tolérance* de l'organisation, quatre stratégies de traitement sont disponibles :

- **Eviter :** les actions visent à empêcher le risque de se réaliser ;
- **Réduire :** le but des actions est de diminuer la probabilité et/ou l'impact des risques, p. ex. de manière préventive en instaurant des contrôles ou en les renforçant, ou en les maîtrisant aussi rapidement et favorablement que possible en appliquant des plans de crise ou de continuité ;

- **Transférer ou partager :** certains risques peuvent être assurés ou externalisés auprès d'entités tierces ;
- **Accepter :** s'il est suffisamment bas ou que les coûts ou efforts d'actions potentielles sont excessifs, ou encore s'il n'existe aucune option réaliste pour le réduire, le risque peut être simplement surveillé, sans qu'aucune autre action ne soit entreprise.

Une autorité décisionnelle est chargée de valider la stratégie de traitement d'un risque et de définir qui en sera *propriétaire*. Elle est déterminée par le niveau de gravité du risque défini précédemment et se situe le plus bas possible dans la hiérarchie. Ceci évite d'une part que trop de risques peu importants soient remontés systématiquement à des niveaux hiérarchiques supérieurs, permettant ainsi de focaliser l'attention sur les risques majeurs. D'autre part, cela empêche qu'à un niveau hiérarchique trop bas, des décisions soient prises sans impliquer le management dans le cadre de risques graves.



Source : Cour des comptes 2013

Il incombe à l'autorité décisionnelle de sélectionner la stratégie de traitement appropriée pour chaque risque identifié. Si le risque n'est pas accepté, des plans d'action doivent être élaborés et documentés. Chaque plan d'action doit avoir un·e responsable désigné·e (*propriétaire du risque*) et un délai précis pour assurer une mise en œuvre efficace.

Le coût de mise en œuvre d'une mesure ne doit pas dépasser les avantages attendus, c'est-à-dire que l'effort fourni (ressources humaines, financières, durée, etc.) doit être équilibré en fonction de la gravité du risque. Les coûts des mesures doivent être inscrits au budget de l'Etat.

L'évaluation et le traitement des risques transversaux

Les risques transversaux, qui peuvent impacter plusieurs départements ou services, doivent être abordés avec une attention particulière. Des mécanismes de coordination sont nécessaires pour évaluer et gérer ces risques. Une approche collaborative favorise une gestion homogène et cohérente qui transcende les frontières organisationnelles, renforçant ainsi la résilience globale de l'administration.

Les directives cantonales doivent inclure la manière de traiter les risques transversaux pour permettre à l'ACV d'identifier et gérer de manière proactive ces risques qui présentent des enjeux importants.

Cela favorise une meilleure compréhension des risques, une prise de décision éclairée et une réduction efficace des impacts négatifs potentiels.

Des exemples pertinents

Des directives pour la *gestion intégrée des risques* revêtent une importance cruciale pour assurer la cohérence et l'efficacité de la GDR à tous les niveaux de l'administration. Elles permettent de concrétiser la stratégie, de garantir une identification exhaustive des risques, une évaluation homogène, ainsi qu'une maîtrise proactive des risques pour atteindre les objectifs.

A titre d'exemple, on peut se référer aux règlements ou directives sur la GDR édictées par d'autres cantons, tels que Genève [27] ou, plus récemment, Berne [28]. Les directives du Canton de Berne mentionnent que, pour tenir compte de la variété et de l'hétérogénéité des situations, il est important d'accorder une certaine latitude aux offices pour organiser la GDR en fonction de leurs besoins spécifiques. En effet, il existe dans certains offices ou domaines de tâches des dispositifs de GDR parfois déjà très complets, qui vont plus loin que les bases et les principes décrits dans ces directives cantonales.

En ce qui concerne l'administration fédérale, différentes directives [29 et 30] constituent une base contraignante pour la GDR menée par les départements et unités administratives. En outre, un Manuel de gestion des risques[31] a été publié (c'est également le cas de l'Etat de Genève) afin de fournir des explications sur la mise en œuvre des directives. Un tel manuel a pour objectif de compléter les directives en décrivant de façon détaillée et opérationnelle les activités à réaliser, les méthodes à appliquer, les bonnes pratiques, etc.

Pour éviter que chaque service et direction générale mette en œuvre de manière non coordonnée un système de GDR, le CE doit rédiger des directives qui définissent le minimum qui est attendu de leur part. Le but est également de valoriser les bonnes pratiques qui existent déjà à l'heure actuelle (p.ex. certification *ISO 9001:2015* de certains services, qui atteste de la mise en place d'un système de GDR formalisé).

Elaborer des directives	
Recommandation n° 2	**au Conseil d'Etat**
Afin d'assurer que les évaluations des différents risques soient réalisées de la même manière et de permettre leur consolidation, rédiger des directives pour que l'ensemble de l'ACV applique des règles homogènes.	

[27] Règlement sur la gestion des risques du 18 septembre 2013.
[28] Directives sur la gestion des risques du Canton de Berne, du 24 novembre 2021.
[29] Directives sur la politique de gestion des risques menée par la Confédération, du 24 septembre 2010.
[30] Directives sur la gestion des risques de la Confédération, Administration fédérale des finances – service juridique, version du 31 mars 2016.
[31] Manuel de gestion des risques de la Confédération, version du 22 mars 2022.

3.1.3. Définir les fonctions, rôles et responsabilités

Dans un système de *gestion intégrée des risques*, chaque acteur joue un rôle essentiel pour assurer la prise en compte systématique des risques à tous les niveaux et pour favoriser une culture de gestion proactive des risques. La GDR ne doit pas être considérée comme un « mal nécessaire », venant se greffer sur les activités opérationnelles de l'organisation : elle est partie intégrante de ces activités. C'est pourquoi la politique et les directives doivent clairement définir les fonctions et responsabilités de chaque niveau hiérarchique, en précisant les tâches spécifiques liées à la GDR au sein de l'ACV. Ces rôles et responsabilités doivent être communiqués à tout le personnel pour s'assurer que chaque personne se sente impliquée pour ses activités propres et les risques y relatifs, ainsi que consciente des interactions entre ses activités et celles des autres.

En se référant à la GDR instaurée dans d'autres administrations publiques, les rôles des différentes parties prenantes au sein de l'ACV pourraient être les suivants :

Les fonctions et responsabilités aux différents niveaux hiérarchiques

Conseil d'Etat

Au niveau le plus élevé, le CE porte la responsabilité globale de la GDR. Il lui reviendrait dès lors d'/de :

- Définir la vision, les objectifs et la stratégie globale et adopter la politique en matière de GDR ;
- Adopter, via des directives, les principes de GDR devant s'appliquer à l'ensemble de l'ACV et comprenant notamment les critères d'évaluation et d'acceptation des risques ;
- Attribuer les moyens nécessaires pour soutenir le lancement de la GDR à l'échelle de l'ACV ;
- Prendre en charge la *gestion des risques* majeurs relevant de son niveau décisionnel et assumer la responsabilité suprême des risques de l'ACV ;
- Évaluer régulièrement les risques globaux auxquels l'Etat est exposé ainsi que le système mis en place dans une démarche d'amélioration continue ;
- Approuver le rapport périodique consolidé sur les risques.

Chef·fe·s de département

Lorsque les risques ne sont pas d'un niveau justifiant de remonter jusqu'au CE, ils sont gérés au niveau de chaque département. Dans ce cas, le ou la chef·fe·de département devrait :

- Veiller à la mise en œuvre d'un système de GDR conforme à la politique générale définie par le CE et intégrer la GDR dans la planification stratégique et les processus décisionnels de son département ;
- Attribuer les moyens appropriés et un soutien adéquat pour la mise en œuvre de la GDR au sein de son département ;
- Identifier et évaluer les risques spécifiques liés à son domaine d'activité ;
- Assumer la responsabilité des risques associés aux tâches qui lui sont confiées ;
- Examiner les mesures de réduction des risques prévues et s'assurer de leur mise en œuvre ;
- Fournir des informations pour le rapport périodique sur les risques.

Directeur·trice·s ou chef·fe·s de services

En descendant encore d'un niveau dans le degré de gravité des risques, les responsables de chaque direction générale et de chaque service devraient :

- Assumer la responsabilité des risques liés à leur domaine d'activité spécifique ;
- Mettre en œuvre les processus de GDR dans leur domaine de compétence conformément aux directives ;
- Si une situation de risque exceptionnelle se présente, en informer le ou la chef·fe de département directement et sans délai ;
- Collaborer avec d'autres entités pour la *gestion des risques* transversaux ;
- Contribuer à l'amélioration continue du système de GDR ;
- Fournir des informations pour le rapport périodique sur les risques.

Le personnel de l'ACV
Chaque collaborateur·trice de l'ACV (employé·e et cadre de tous niveaux), conformément à son cahier des charges, devrait :

- Participer activement à la GDR en signalant les risques et en mettant en œuvre les mesures de prévention appropriées ;
- Se conformer aux politiques et aux directives en matière de GDR et gérer les risques pour lesquels la personne a été désignée *propriétaire*.

Les rôles et responsabilités des fonctions transversales

Pour garantir, au niveau de l'ACV, la consolidation des risques principaux et une mise en œuvre aussi uniforme que possible, différentes tâches transversales doivent être effectuées, notamment :

- Coordonner les rapports sur les risques provenant des différents services ; consolider les informations par département, puis globalement au niveau de l'ACV, notamment pour les intégrer dans les rapports périodiques ;
- Identifier les risques transversaux à l'échelle de l'ACV, analyser les interactions possibles entre les risques des départements, les consolider et définir un ordre de priorité ;
- Sélectionner les mesures appropriées et proposer au CE d'accepter formellement les *risques résiduels* ;
- Choisir et assurer la mise à disposition d'une application informatique unique pour la GDR de l'ACV ;
- Suivre l'application des directives en matière de GDR aux différents niveaux de l'ACV ;
- Apporter un soutien technique et méthodologique aux *propriétaires des risques* ;
- Favoriser l'amélioration continue, notamment par l'échange de bonnes pratiques ;
- Faciliter la communication et la collaboration entre les différentes entités impliquées ;
- Evaluer régulièrement l'efficacité globale de la GDR dans l'ACV et proposer les améliorations nécessaires au CE.

Au sein de l'ACV, la CHA et les secrétaires généraux exercent des fonctions transversales. De plus, des services traitent de problématiques transversales dans des domaines spécifiques, afin d'identifier, d'évaluer et de gérer les risques pour des activités regroupées au niveau cantonal : p.ex. bâtiments (DGIP), informatique (DGNSI), ressources humaines (DGRH) et finances (SAGEFI).

Les rôles et responsabilités en matière de GDR de ces fonctions et services doivent être précisés afin de s'assurer que les tâches transversales susmentionnées sont réalisées. Le but est d'harmoniser et

d'agréger ces risques pour l'ensemble de l'ACV, en collaborant avec les directions générales et les services pour une approche intégrée de la GDR.

En outre, une entité centrale devrait être désignée pour consolider l'ensemble des risques principaux et assurer la coordination globale de la GDR au sein de l'ACV.

Afin d'assurer une cohérence de la GDR dans l'ensemble de l'ACV, une consolidation des risques transversaux et une remontée des informations aux niveaux adéquats, il est nécessaire de définir les rôles et responsabilités des différent·e·s intervenant·e·s. C'est pourquoi la recommandation suivante est formulée.

Définir les fonctions, rôles et responsabilités	
Recommandation n° 3	**au Conseil d'Etat**
a) Définir les fonctions, rôles et responsabilités en matière de *gestion des risques*, y compris en ce qui concerne l'agrégation et la gestion des risques transversaux, pour les acteurs de l'ACV à tous les échelons hiérarchiques. b) Désigner une entité responsable de la coordination du système, de l'analyse des interactions ainsi que de la centralisation des risques principaux des départements et des risques transversaux pour transmission au CE.	

3.1.4. Poursuivre les démarches initiées

La certification des SCI

Lors du démarrage du présent audit, la Cour a appris que le CE avait demandé au Contrôle cantonal des finances (CCF) de préparer une présentation et une appréciation générale sur l'implémentation des SCI au sein de l'ACV, une fois les attestations délivrées. Cette présentation a permis d'évaluer la possibilité de l'application d'un SCI plus large étendu aux prestations et à une *gestion intégrée des risques* à l'État de Vaud, en se basant notamment sur l'expérience du SSCM pour l'analyse des risques dans le domaine de la protection de la population. Sur ces bases, le CE a pu envisager une démarche pour le déploiement interne d'un système de GDR.

Le lancement d'une étude préliminaire

Le CE a confirmé à la Cour que la thématique de la GDR reste au cœur de l'actualité. Cependant, le CE juge qu'il est crucial d'éviter la mise en place de solutions disparates au sein de l'ACV. Une telle approche entrerait en contradiction avec les objectifs énoncés dans le cadre du programme de législature 2022-2027, qui vise à renforcer la transversalité de l'action publique et la résilience du canton, notamment en matière de prévention des risques et de gestion de crise. Afin d'éviter une telle situation, le CE envisage de développer une solution coordonnée et pragmatique pour la mise en place d'un système de *gestion intégrée des risques*, qui tienne aussi compte des moyens et ressources à mobiliser à cette fin. Il a toutefois relevé que cette approche nécessite de définir le périmètre retenu, de fixer le degré d'acceptation du risque et d'obtenir l'adhésion de l'ensemble de l'ACV.

Le CE a d'ores et déjà décidé de mandater un prestataire externe pour réaliser une analyse préalable, portant sur les systèmes existants dans d'autres collectivités publiques (Confédération, cantons,

communes), les différentes méthodes de GDR, la possibilité d'intégrer les dispositifs existants de l'ACV (SCI, certifications ISO…), ainsi que les moyens matériels et humains à mettre en œuvre. Les résultats de cette étude devraient être connus en février 2024.

Sur la base de cette étude préliminaire, le CE devra déterminer le périmètre retenu et allouer les ressources nécessaires pour le développement de la GDR au sein de l'ACV. Le CE envisage de lancer un appel d'offres pour désigner un prestataire pour l'accompagner dans ce projet.

La responsabilité des premières démarches a été attribuée à la CHA. Le collège des secrétaires généraux sera l'organe de coordination et d'échange d'information pour le lancement et le suivi du dossier.

3.2. Mettre en œuvre la gestion des risques définie

Pour instaurer une *gestion intégrée des risques* pour l'ensemble de l'ACV conforme à la politique et aux directives qu'il aura définies, le CE devra agir dans les domaines suivants :

- Etablir un plan d'action ;
- Collecter, consolider et gérer les risques ;
- Assurer la communication nécessaire.

3.2.1. Etablir un plan d'action

L'élaboration d'un plan d'action constitue la première étape essentielle pour implémenter de manière efficiente une *gestion intégrée des risques* au sein de l'ACV. Ce plan visera à identifier les activités nécessaires à l'instauration du système défini de GDR, tout en attribuant des responsabilités spécifiques à chaque catégorie d'acteurs et en planifiant les principales étapes. L'objectif principal de ce plan est de servir de guide pour l'amorçage du processus de GDR, en mettant en avant les jalons clés à atteindre et des indicateurs pour mesurer l'avancement.

Parallèlement, l'allocation adéquate de moyens, qu'ils soient financiers, humains ou technologiques, se révèle primordiale pour la réalisation fluide du plan d'action. Ils doivent être correctement dimensionnés pour soutenir la mise en place du système de GDR.

Finalement, pour instaurer une culture de la GDR au sein de l'administration, il est crucial de former et de sensibiliser les cadres et le personnel aux avantages de cette approche dans les processus décisionnels et dans l'exécution des activités. L'intégration de l'évaluation des risques dans les décisions, les projets et les stratégies administratives garantira ainsi une approche réfléchie et proactive face aux incertitudes inhérentes aux activités de l'ACV.

3.2.2. Collecter, consolider et gérer les risques

La collecte, la consolidation et la gestion des risques à proprement parler constituent la pierre angulaire de la mise en œuvre du système de GDR. Il s'agit de systématiquement identifier, évaluer et gérer au bon niveau les divers risques qui peuvent affecter le bon fonctionnement de l'ACV.

Lorsque le système de GDR aura démarré, le CE devra s'assurer que les différentes directions générales et services mettent en œuvre ce qu'il aura défini au travers de la stratégie (cf. 2.3.1.) et des directives (cf. 2.3.2.).

Collecte et remontée des informations au bon niveau hiérarchique

La collecte d'informations concernant l'identification des risques, les mesures d'atténuation et les éventuels problèmes rencontrés est un processus méthodique et rigoureux à tous les niveaux de l'organisation. Chaque niveau hiérarchique joue un rôle essentiel pour garantir une remontée régulière et structurée des informations aux niveaux supérieurs, selon la gravité définie des menaces identifiées.

En facilitant la transmission de données pertinentes aux niveaux adéquats, les décideur·euse·s sont alors en mesure de prendre des décisions tenant compte des risques. En outre, la communication favorise la sensibilisation collective et assure une gestion proactive des risques à tous les niveaux de l'organisation.

Consolidation des risques transversaux

Après la collecte des données relatives aux risques, la consolidation vise à agréger les risques individuels en vue de fournir une vision globale, permettant ainsi une meilleure appréhension des risques auxquels une ou plusieurs entités peuvent être exposées. L'agrégation devrait être entreprise uniquement lorsque cela apporte une valeur ajoutée significative.

Dans le cadre de l'agrégation, il est essentiel de clarifier les interdépendances et les interactions entre les risques. Les entités désignées comme responsables de la consolidation ou du traitement des risques transversaux (voir chapitre 3.1.3) sont chargées de superviser ces aspects essentiels.

Gestion proactive des risques

Pour chaque risque identifié, des stratégies d'atténuation spécifiques sont élaborées, dans le but de réduire les probabilités d'occurrence et de minimiser les répercussions négatives en cas de réalisation. Il incombe aux directions concernées de veiller à la mise en place effective des mesures de prévention conformément à la planification. Cette approche proactive permet de garantir une réaction efficace et une réduction des impacts potentiels.

3.2.3. Assurer la communication nécessaire

Objectifs de la communication et du reporting en matière de GDR

La communication interne et externe, ainsi que le reporting, jouent un rôle essentiel dans la *gestion intégrée des risques*. Une communication bien structurée permet une analyse approfondie des risques en s'appuyant sur les meilleures connaissances spécialisées disponibles. Elle assure également la prise en compte des intérêts et des avis de toutes les parties prenantes, renforçant ainsi leur confiance. Enfin, le système de reporting doit assurer une remontée fluide de l'information aux échelons hiérarchiques appropriés, favorisant ainsi une prise de décision éclairée.

Pour atteindre ces objectifs, les directives doivent définir clairement les responsabilités de chaque partie prenante dans la communication et le reporting des risques et des mesures prises. Elles doivent spécifier les canaux de communication à utiliser (p. ex. réunions, rapports écrits, intranet ou courriels)

en fonction des besoins de l'organisation. De plus, il convient de préciser la fréquence minimale des mises à jour, englobant à la fois les risques existants et les nouveaux risques identifiés.

Outils de communication

L'utilisation d'outils informatiques peut grandement soutenir une mise en œuvre homogène du processus de GDR au sein de l'organisation, tout en facilitant la préparation de rapports destinés aux autorités, au public et aux parties prenantes externes. Idéalement, la GDR devrait reposer sur un système d'information, si possible interconnecté avec les autres systèmes de l'organisation, afin de permettre une gestion fluide et performante des données.

L'audit réalisé en 2013 avait relevé que la Direction des Systèmes d'Information (DSI) utilisait une solution logicielle pour élaborer des schémas directeurs métier, comprenant notamment un module dédié à la GDR. Depuis, l'application SIEL a été déployée et adoptée par tous les services de l'ACV. Cette plateforme permet déjà de suivre les éléments traités par le CE et le Grand Conseil.

Afin de simplifier la GDR, il est crucial de sélectionner et déployer les outils technologiques nécessaires pour collecter, surveiller et évaluer les risques de manière efficiente. L'administration fédérale, à titre d'exemple, fait usage d'un logiciel baptisé Risk to Chance (R2C), qui est spécifiquement conçu pour la GDR. Il permet de :

- Recenser et documenter les risques ;
- Enregistrer les mesures et évaluer leur niveau de mise en œuvre ;
- Enregistrer les dommages subis et les enseignements tirés lorsque des risques se réalisent ;
- Générer des rapports sur les risques.

Communication interne

Afin d'instaurer un système de GDR de manière efficace et efficiente, il est essentiel d'établir une communication régulière entre les divers départements et services de l'ACV, et d'assurer une remontée d'informations concernant les progrès accomplis dans la mise en œuvre de la GDR.

Les collaborateur·trice·s de l'ACV doivent être sensibilisé·e·s aux enjeux inhérents à la GDR ainsi qu'à leur rôle dans ce domaine. Dans cette optique, il est primordial d'établir des dispositifs favorisant la communication tels que la formation du personnel, des canaux simples de signalement ainsi que des mécanismes de rétroaction appropriés.

Une communication fluide assure la transmission régulière d'informations aux échelons décisionnels appropriés et renforce la confiance envers les mécanismes de GDR mis en place. Cette approche contribue à une culture de la transparence et de la responsabilité au sein de l'organisation.

Communication externe

La communication externe doit être transparente, tout en veillant à préserver la confidentialité des informations sensibles. Il s'agit donc de définir clairement ce qui devrait être communiqué, ou au contraire être considéré comme confidentiel, pour des raisons de sécurité. Les inventaires des risques et des contrôles sont généralement classés comme « non-publics ». Les rapports doivent inclure des éléments clés tels que l'identification des risques, leur évaluation, les mesures d'atténuation en place, les progrès réalisés et les responsabilités attribuées.

Il est également nécessaire d'instaurer une communication externe ciblée. Il convient, en amont, de prendre en compte des informations résultant de la consultation des parties prenantes, notamment concernant les évolutions contextuelles. Puis, en aval, d'informer les parties prenantes appropriées sur les mesures adoptées pour gérer les risques et assurer la continuité des prestations à la population.

Reporting — rapports périodiques

La fréquence et le contenu des rapports doivent être clairement définis par les directives. Certains éléments essentiels doivent être inclus, tels que la description des risques principaux avec leurs causes, conséquences et évaluations, des visualisations graphiques pour une vue d'ensemble ainsi que la tendance au fil du temps, et des indicateurs de performance de la GDR pour évaluer l'efficacité des stratégies d'atténuation.

La consolidation des risques est également un élément clé de communication, souvent intégré dans les rapports. Elle permet une lecture facile et une vue d'ensemble synthétique des risques, en particulier pour certains aspects spécifiques.

Un système de reporting régulier doit donc être mis en place. Ce système permet, d'une part, de fournir une vue d'ensemble de la situation à la hiérarchie et, d'autre part, d'informer les parties prenantes concernées. Ce processus se matérialise par la création de rapports périodiques qui détaillent les risques identifiés, leur évaluation, leur évolution et les mesures prises pour les gérer. Il peut être intéressant d'y intégrer une visualisation graphique des risques consolidés, ce qui permet de simplifier l'appréciation et de mettre en lumière des aspects spécifiques. Idéalement, ces rapports périodiques devraient pouvoir être générés dans le système d'information défini.

Ces trois étapes faciliteront la mise en œuvre de la *gestion intégrée des risques* au sein de l'administration cantonale vaudoise. Le suivi, l'évaluation et l'amélioration continue pourront alors être entrepris pour améliorer continuellement le système de GDR.

Mettre en œuvre la *gestion des risques* définie	
Recommandation n° 4	**au Conseil d'Etat**
a) Etablir un plan d'action pour le déploiement de la GDR dans l'ensemble de l'ACV. b) Mettre en place des mécanismes réguliers de collecte, d'évaluation, de consolidation et d'agrégation des risques afin de maintenir une vision actualisée des risques auxquels l'Etat de Vaud est confronté, en accordant une attention particulière aux risques les plus critiques ou ayant un impact potentiel élevé et en tenant compte des interactions entre les risques. c) Assurer la communication interne et externe nécessaire, notamment au moyen de rapports explicatifs réguliers sur les risques.	

3.3. Instaurer un suivi et une amélioration continue

Le concept d'amélioration continue est au cœur de la philosophie de GDR. Cela inclut une analyse régulière et des mises à jour afin d'adapter le système en fonction des enseignements tirés de l'expérience acquise. L'objectif est d'assurer que le système de GDR demeure pertinent et efficace au fil du temps, en tenant compte des évolutions du contexte et des nouveaux défis auxquels

l'organisation est confrontée. Cette démarche d'amélioration continue vise à optimiser la performance du système de GDR, en identifiant les points forts à conserver et en apportant des ajustements pour corriger d'éventuelles faiblesses.

La personne *propriétaire du risque* est chargée de surveiller les risques et les mesures, assurant ainsi une gestion proactive et efficace des risques dans l'organisation.

La fréquence de mise à jour minimale du portefeuille des risques ainsi que celle des mesures prévues et des plans d'action doivent être définies dans les directives : p. ex. annuellement, voire plus fréquemment pour les risques principaux ou lors de changements importants, selon le principe de proportionnalité. Ceci est particulièrement important pour les plans d'action, car le suivi de leur état est essentiel pour que la GDR déclenche toute sa valeur ajoutée et pour permettre une mesure correcte des indicateurs de performance.

3.3.1. Surveiller les risques et les mesures

La surveillance continue des risques et des mesures entreprises revêt une importance capitale dans le processus de GDR, car elle assure l'efficacité de ce processus tout en maximisant sa valeur en tant qu'outil d'aide à la décision.

La surveillance des risques

Une surveillance est essentielle pour s'assurer que les connaissances relatives aux risques sont à jour. Elle vise à identifier les changements qui pourraient affecter l'appréciation des risques existants et à détecter précocement de nouveaux risques. Il s'agit de mettre à jour les informations sur les risques (ainsi que sur les contrôles les concernant) ou de confirmer que la documentation ne nécessite pas de changements. Cette responsabilité incombe principalement aux *propriétaires des risques*.

De plus, le portefeuille doit être régulièrement réévalué pour s'assurer que sa taille est raisonnable, c'est-à-dire que le nombre de risques n'est pas trop élevé pour assurer une gestion efficiente. Il faut aussi s'assurer que tous les risques importants figurent dans la matrice des risques et que des responsables ont été désigné·e·s (*propriétaires des risques*).

La surveillance des mesures

La surveillance des mesures de prévention ou de réduction des risques est également primordiale. Il s'agit d'évaluer si les mesures prévues sont encore adéquates ou si les conditions ont évolué.

En outre, les *propriétaires de risques* sont responsables de s'assurer que les mesures sont mises en œuvre dans les délais, en respectant les budgets prévus et qu'elles atteignent leurs objectifs. Ils doivent aussi fournir des rapports sur les progrès réalisés et les problèmes éventuellement rencontrés lors de la mise en œuvre.

La performance globale de la GDR peut être évaluée en mettant en place et en analysant des indicateurs clés tels que le taux de traitement des risques, le niveau de conformité aux politiques, ou encore la réduction des impacts liés aux risques. Ces indicateurs fournissent une vue d'ensemble précieuse de l'efficacité du système de GDR. En utilisant ces données, des plans d'action peuvent être développés et mis en œuvre pour remédier aux lacunes identifiées. Cette démarche permet non seulement de renforcer la résilience de l'organisation face aux risques, mais aussi d'optimiser ses

processus. Elle contribue ainsi à garantir la stabilité et la pérennité de l'entité tout en favorisant une culture d'amélioration continue.

En particulier le suivi des plans d'action représente un élément fondamental pour que la GDR soit utilisée effectivement comme outil de pilotage dynamique. Si elle n'est pas accompagnée par un suivi régulier des plans d'action, la simple mise à jour de la documentation sur les risques pourrait perdre de sa pertinence et affaiblir de manière significative l'efficacité du processus.

3.3.2. Améliorer l'organisation du système

Une évolution constante pour une gestion proactive des risques

Une fois le système de GDR en place, son évolution permanente est essentielle pour maintenir sa pertinence et son efficacité. Un système statique est insuffisant ; il doit s'adapter aux défis changeants auxquels l'organisation est confrontée. Une évaluation régulière permet de déterminer dans quelle mesure le système de GDR est mis en œuvre et s'il fonctionne conformément aux objectifs définis.

Pour identifier des opportunités d'amélioration et optimiser la GDR, l'ACV peut s'appuyer sur des informations internes issues des retours d'expérience et des pratiques passées, ainsi que sur des informations externes. Ces éléments permettent d'ajuster les directives et le manuel de GDR, notamment pour les aligner avec les normes et les directives internationales les plus récentes.

En adoptant une approche itérative et proactive, l'organisation renforce sa capacité à anticiper et à répondre aux nouveaux risques et aux défis émergents. Cette culture d'amélioration continue rend l'organisation plus résiliente, capable de s'adapter rapidement aux changements, et assure une GDR optimale au bénéfice de l'ensemble de l'ACV et de ses parties prenantes.

Apprendre des erreurs

L'analyse des erreurs et des défauts constatés peut être utilisée pour évaluer et améliorer la *gestion des risques* existants et émergents.

En 2009, l'*International Risk Governance Council* (IRGC)[32] a identifié deux catégories principales de défauts dans les processus et structures de GDR :

- Erreurs ou biais dans l'évaluation et la compréhension des risques, qui peuvent découler d'un manque de connaissances, de problèmes dans les processus de collecte, d'analyse et de communication des données, ou encore résulter de la complexité et des interdépendances au sein du système.
- Défauts dans le traitement des risques, se manifestant par des faiblesses dans :
  a) la préparation et la prise de décision concernant les stratégies et les politiques de GDR ;
  b) la formulation de réponses et la prise de mesures ;
  c) les capacités organisationnelles de mise en œuvre des mesures et de suivi de leurs incidences.

[32] Report — Risk Governance Deficits An analysis and illustration of the most common deficits in risk governance, IRGC, 2009, https://irgc.org/risk-governance/irgc-risk-governance-deficits/

Ces défauts doivent être corrigés pour éviter des conséquences coûteuses, ou à l'inverse, le gaspillage de ressources engendré par des mesures excessives ou inefficaces. De plus, ils risquent de diminuer la confiance du public et entraîner une répartition injuste des risques et des bénéfices.

L'analyse des erreurs vise à identifier les lacunes significatives dans les structures et processus de GDR. Tirer des leçons des erreurs passées permet de développer des mesures correctives et s'assurer que le système s'adapte efficacement aux nouveaux défis et enjeux.

Pour s'assurer que le système de GDR fonctionne conformément aux attentes, ne devienne pas obsolète et s'adapte aux évolutions de l'ACV et de son environnement, il est nécessaire d'instaurer des processus de mise à jour et d'amélioration continue.

Instaurer un suivi et une amélioration continue	
Recommandation n° 5	**au Conseil d'Etat**
Exercer un suivi régulier et identifier les lacunes ou les opportunités d'amélioration et prendre des mesures d'amélioration appropriées : a) Mettre à jour les procédures et les processus de *gestion des risques*. b) S'assurer que le portefeuille des risques remontant au CE contient tous les risques importants (mais pas plus) et que les nouveaux risques sont pris en considération. c) S'assurer que les mesures prévues sont adéquates et que leur mise en œuvre permet de réduire efficacement les risques.	

4. Conclusion

Dix ans après son dernier rapport dans le domaine de la *gestion des risques* (GDR), la Cour a décidé de relancer un audit, conformément à la mission qui lui est spécifiquement attribuée à l'article 4 alinéa 1b de la loi sur la Cour des comptes (LCComptes) :

> ***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 mission implique deux conditions préalables : l'existence d'une GDR et son évaluation régulière. Les travaux de la Cour sont destinés à valider l'existence et à évaluer la pertinence du processus de GDR mis en place par l'entité pour gérer les risques de ses activités.

Relevant que le CE vaudois entendait d'abord assurer l'implémentation d'un *Système de contrôle interne* (SCI) dans tous les services de l'ACV, la Cour a décidé d'arrêter le suivi des recommandations émises en 2013, qui demandaient principalement la mise en place d'une *gestion intégrée des risques*, conformément aux principes de bonne gouvernance du secteur public.

L'implémentation du SCI a représenté un travail de longue haleine, qui ne s'est terminé que dans le courant de l'année 2023. Couplé avec l'arrivée du nouveau système d'information financier (SAP), le SCI a permis de réaliser une *cartographie globale des risques* financiers, voire de certains risques de conformité, une première étape importante pour la GDR. Dans son rapport sur les comptes 2022, le CCF a d'ailleurs pu attester, pour la première fois, l'existence d'un SCI relatif à l'établissement des comptes de l'Etat de Vaud.

D'autres jalons ont également marqué ces dernières années dans l'approche de la GDR :

- Politique générale de sécurité des systèmes d'information et analyse des risques de sécurité informatique ;
- *Gestion intégrée des risques* naturels ;
- Analyse des risques pour la protection de la population ;
- Gestion de la crise COVID ;
- Plan de continuité en cas de pénurie énergétique.

Un élément est en revanche resté immuable, à savoir l'absence de définition par le CE d'une politique cantonale en matière de GDR, ce qui rend délicate pour la Cour la mission légale de devoir vérifier ce qui n'existe généralement pas.

Consciente ainsi que les conclusions d'un audit seraient certainement similaires à ceux des précédents audits 2010 et 2013, la Cour a fixé deux objectifs complémentaires à ce nouvel audit :

- Faire un état des lieux de la GDR en examinant les pratiques d'une sélection de services ;
- Evaluer la sensibilité à l'importance d'une *gestion intégrée des risques* au sein des services audités.

Dans un souci d'exemplarité, six services ont été sélectionnés pour cet audit : deux directions avec un budget et un nombre d'ETP d'importance significative, deux entités transversales et deux services déjà inclus dans l'audit de 2013 sur la *gestion intégrée des risques*. La Cour a toutefois pris l'option de ne pas diffuser la notation de cette évaluation.

Appréciation de la Cour

A l'instar des constatations faites en 2010 et 2013, il n'existe toujours pas à ce jour de stratégie définissant la GDR voulue pour l'ACV. Même si la GDR fait partie des principes de bonne gouvernance, plusieurs services audités ont ainsi mentionné qu'ils n'avaient pas mis en place ce qui ne leur était pas demandé. Certains services ont toutefois lancé des démarches qualité et obtenu des certifications de type ISO ou autres, qui incluent les éléments nécessaires en matière de GDR.

Malgré l'absence de référentiel cantonal, les entités prennent toutes en compte les risques dans leurs pratiques quotidiennes. Elles ont aussi une bonne perception des risques opérationnels, directement liés à leurs prestations. Certaines procédures sont déjà formalisées et permettent l'évaluation et le traitement de risques spécifiques. Des dispositions favorables existent certes, mais les risques ne sont pas abordés de manière systématique et pas nécessairement liés aux objectifs.

Les interactions entre les différents risques ne sont pas prises en considération et les risques transversaux ne sont pas agrégés. Par conséquent, le CE ne dispose pas d'une vision globale pour l'ensemble de l'Etat, ni même par département, qui pourrait favoriser une meilleure prise de décision.

Afin de remédier à ces pratiques non harmonisées et peu, voire pas, formalisées pour certains services, il est nécessaire que le CE définisse une vision globale et donne les impulsions nécessaires à la mise en place d'une véritable *gestion intégrée des risques* pour l'ensemble de l'ACV.

En conclusion, la Cour n'adresse des recommandations qu'au CE ; elles visent pour l'essentiel à cadrer la mise en place d'une GDR au niveau cantonal :

1. Définir une *gestion intégrée des risques* pour l'ACV, notamment une politique homogène
2. Elaborer les directives nécessaires (identification, analyse et traitement, communication)
3. Définir les fonctions et responsabilités, assurer notamment la désignation de *propriétaires* pour tous les risques identifiés
4. Mettre en œuvre ensuite cette GDR cantonale définie
5. Instaurer enfin un suivi et une amélioration continue

La Cour adresse ainsi cinq recommandations au CE, qui s'intègrent parfaitement à la mesure 3.18 du programme de législature 2022-2027 : « Renforcer la transversalité de l'action publique et la résilience du Canton, notamment en matière de prévention des risques et de gestion de crise ».

Ces cinq recommandations sont acceptées.

5. Liste des recommandations et remarques

5.1. Liste des recommandations et position du Conseil d'Etat

Définir une politique cantonale homogène			**Page 34**
Recommandation n° 1			
Elaborer une stratégie formelle en matière de *gestion des risques* visant une approche commune pour l'Etat de Vaud qui inclut la gestion de l'ensemble des risques qui peuvent influer sur la réalisation des mesures figurant dans le programme de législature et des objectifs opérationnels au sein des différents services de l'Etat.			
Position du Conseil d'Etat	☒ Acceptée	☐ Refusée	
Justification (uniquement en cas de refus) :			

Elaborer des directives			**Page 38**
Recommandation n° 2			
Afin d'assurer que les évaluations des différents risques soient réalisées de la même manière et de permettre leur consolidation, rédiger des directives pour que l'ensemble de l'ACV applique des règles homogènes.			
Position du Conseil d'Etat	☒ Acceptée	☐ Refusée	
Justification (uniquement en cas de refus) :			

Définir les fonctions, rôles et responsabilités			**Page 41**
Recommandation n° 3			
a) Définir les fonctions, rôles et responsabilités en matière de *gestion des risques*, y compris en ce qui concerne l'agrégation et la gestion des risques transversaux, pour les acteurs de l'ACV à tous les échelons hiérarchiques. b) Désigner une entité responsable de la coordination du système, de l'analyse des interactions ainsi que de la centralisation des risques principaux des départements et des risques transversaux pour transmission au CE.			
Position du Conseil d'Etat	☒ Acceptée	☐ Refusée	
Justification (uniquement en cas de refus) :			

Mettre en œuvre la *gestion des risques* définie	**Page 45**
Recommandation n° 4	
a) Etablir un plan d'action pour le déploiement de la GDR dans l'ensemble de l'ACV. b) Mettre en place des mécanismes réguliers de collecte, d'évaluation, de consolidation et d'agrégation des risques afin de maintenir une vision actualisée des risques auxquels l'Etat de Vaud est confronté, en accordant une attention particulière aux risques les plus critiques ou ayant un impact potentiel élevé et en tenant compte des interactions entre les risques. c) Assurer la communication interne et externe nécessaire, notamment au moyen de rapports explicatifs réguliers sur les risques.	
Position du Conseil d'Etat ☒ Acceptée ☐ Refusée	
Justification (uniquement en cas de refus) :	

Instaurer un suivi et une amélioration continue	**Page 48**
Recommandation n° 5	
Exercer un suivi régulier et identifier les lacunes ou les opportunités d'amélioration et prendre des mesures d'amélioration appropriées : a) Mettre à jour les procédures et les processus de *gestion des risques*. b) S'assurer que le portefeuille des risques remontant au CE contient tous les risques importants (mais pas plus) et que les nouveaux risques sont pris en considération. c) S'assurer que les mesures prévues sont adéquates et que leur mise en œuvre permet de réduire efficacement les risques.	
Position du Conseil d'Etat ☒ Acceptée ☐ Refusée	
Justification (uniquement en cas de refus) :	

5.2. Remarques du Conseil d'Etat

canton de vaud
LIBERTÉ PATRIE

CONSEIL D'ETAT

Château cantonal
1014 Lausanne

Cour des comptes
Monsieur Guy-Philippe Bolay
Vice-président
Rue Langallerie 11
1014 Lausanne

Réf. : 23_COU_6935

Lausanne, le 29 novembre 2023

Audit de la gestion intégrée des risques

Monsieur le Vice-président,

Le Conseil d'Etat a pris connaissance de votre projet de rapport et vous remercie de l'avoir consulté. Il a l'avantage de vous faire part ci-dessous de sa prise de position sur les résultats de l'audit et sur les recommandations qui lui sont adressées.

Le Conseil d'Etat salue la qualité du travail de la Cour des Comptes et relève que cet audit illustre de manière équilibrée différents états de développement de la gestion et de l'appétence aux risques dans les multiples composantes de l'administration. Le choix des entités auditées laisse transparaître de manière éloquente la diversité des missions de l'Etat et des défis que représente la gestion des risques à l'échelle de l'Administration cantonale vaudoise. (ACV) Sur la base du constat que vous opérez, il approuve en particulier le fait de ne pas formuler de recommandations aux services, mais de les réserver au Gouvernement.

Ainsi que vous le relevez avec pertinence, le Programme de législature 2022-2027 du Conseil d'Etat prévoit à sa mesure 3.18 de *renforcer la transversalité de l'action publique et de la résilience du Canton, notamment en matière de prévention des risques et de gestion de crise*. Ce faisant et vous le soulignez également, le Conseil d'Etat a décidé de faire réaliser une analyse préalable portant sur les systèmes existant au sein d'autres collectivités publiques, sur les différentes méthodes de gestion intégrée des risques et sur la possibilité d'intégrer les dispositifs d'ores et déjà implantés au sein de l'ACV.

Il est également utile de rappeler à ce stade que, d'une part, l'ensemble de l'administration dispose désormais de SCI financiers et que, d'autre part, toutes les Directions générales et tous les Services ont développé et mis en œuvre des plans de continuité durant toute la crise du COVID et qu'au surplus ces plans ont désormais été adaptés à la prévention des effets d'une crise énergétique potentiellement invalidante pour l'action de l'Etat. La culture de la prévention du risque est donc bien présente au sein de l'ACV, sous une forme qui mérite certes d'être consolidée et unifiée, et le Conseil d'Etat relève avec satisfaction que la progression enregistrée dans ce domaine est substantielle depuis le 1er audit réalisé par la Cour des comptes en 2013.

CONSEIL D'ETAT
www.vd.ch – T 41 21 316 41 59

CONSEIL D'ETAT

Sur le fond, le Conseil d'Etat peut souscrire à l'ensemble des recommandations qui lui sont adressées en tant qu'elles détaillent les différentes étapes de l'adoption, de l'implantation et du suivi d'un système de gestion des risques à l'échelle de l'ACV. Bien que se fondant sur une position de principe, le Conseil d'Etat réserve sa marge de manœuvre dans le choix du système le plus adapté aux besoins de l'administration et du Gouvernement, dans le périmètre à considérer et surtout dans les moyens financiers et les ressources à mobiliser pour déployer le système qui sera finalement adopté. Il souligne à cet égard que le principe d'économicité entrera pour une bonne part dans le processus de choix qui aboutira à l'adoption d'un système de gestion des risques adapté à ses besoins.

Vous remerciant à nouveau de l'avoir consulté et demeurant à votre disposition, le Conseil d'Etat vous prie de croire, Monsieur le Vice-président, à l'assurance de sa considération distinguée.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER a.i.
Christelle Luisier Brodard	François Vodoz

CONSEIL D'ETAT
www.vd.ch – T 41 21 316 41 59

5.3. Remarques des entités auditées

canton de vaud

Service des automobiles et de la navigation

Direction

Av. du Grey 110
1014 Lausanne

Cour des comptes
M. Guy-Philippe Bolay, magistrat
Rue de Langallerie 11
1014 Lausanne

Réf. : DCIRH/SAN/PCY/EFE

Lausanne, le 13 novembre 2023

Audit de la gestion intégrée des risques – Analyse comparative dans six entités de l'administration cantonale vaudoise

Monsieur,

Le projet de rapport mentionné en titre m'est bien parvenu et a retenu toute mon attention.

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

Restant à disposition en cas de besoin, je vous adresse, Monsieur, mes meilleures salutations.

Pascal Chatagny
Chef de service

Copie : SG-DCIRH

Service des automobiles et de la navigation
www.vd.ch/san – T + 41 21 316 89 67 – info.auto@vd.ch

canton de vaud

Le Chef du
Service pénitentiaire

Chemin de l'Islettaz
Bâtiment A
1305 Penthalaz

Cour des comptes
M. Guy-Philippe Bolay, Vice-président
Rue de Langallerie 11
1014 Lausanne

Réf. : RBD, ANN

Penthalaz, le 20 novembre 2023

Audit de la gestion intégrée des risques au sein du Service pénitentiaire – Cour des comptes

---

Monsieur le Vice-président,

En référence à l'envoi du 2 novembre 2023 relatif au rapport d'audit susmentionné et sollicitant une prise de position officielle du SPEN, je me permets vous apporter les éléments suivants.

D'une manière générale, je tiens tout d'abord à relever l'efficacité et la fluidité des échanges que nous avons eus avec la Cour des comptes depuis le début de la démarche, soit il y a une année. La gestion des risques fait intégralement partie de notre mission régalienne et guide bon nombre de nos processus. Ces échanges structurés et constructifs nous ont permis de nous situer par rapport aux exigences d'une gestion intégrée des risques que je souhaite développer encore davantage au sein de mon service. Comme déjà exprimé notamment par courriel, je partage ainsi pleinement le sens des missions que vous recommandez de confier aux services en matière de gestion des risques.

D'un point de vue plus particulier, je n'ai pas de commentaire supplémentaire à formuler sur les recommandations de la Cour.

En réitérant mes remerciements, je vous prie d'agréer, Monsieur le Vice-président mes respectueuses salutations.

RBB

Raphaël Brossard
Chef de service

Service pénitentiaire – Département de la jeunesse, de l'environnement et de la sécurité
www.vd.ch/spen – T + 41 21 316 48 01 – info.spen@vd.ch

canton de vaud

Direction générale de l'emploi et du marché du travail - DGEM

Rue Caroline 11
1014 Lausanne

Cour des Comptes du Canton de Vaud
Monsieur Guy-Philippe Bolay
Vice-Président
Rue de la Langallerie 11
1014 Lausanne

Également transmis par courriel

Lausanne, le 22 novembre 2023

Rapport d'audit n°81 de la Cour des Comptes : gestion intégrée des risques

Monsieur le Vice-Président,

Nous vous remercions de nous avoir transmis pour détermination votre rapport relatif à la gestion intégrée des risques, étant entendu que la Direction générale de l'emploi et du marché du travail (DGEM) figurait au rang des six entités auditées.

Nous avons procédé à une lecture attentive de votre document. Vos recommandations s'adressant directement au Conseil d'Etat, nous nous limiterons à relever ce qui suit.

La DGEM constate avec satisfaction que la Cour des Comptes défend une approche uniformisée de la gestion intégrée des risques et, qu'à ce titre, elle en appelle au Conseil d'Etat pour définir le cadre et les moyens de sa mise en œuvre au sein de l'Administration cantonale. Comme vous le notez effectivement, l'approche actuelle est parcellaire et repose sur les exigences, compétences et contraintes propres à chaque service. C'est ainsi que pour la DGEM, comme vous le mentionnez en pages 22 à 24 du rapport, le degré de maturité des différentes entités se révèle variable.

Ainsi, nous nous réjouissons à cet égard que votre rapport mette en lumière la certification ISO 9001 : 2015 de la Caisse cantonale de chômage (CCh), laquelle vient d'ailleurs d'être renouvelée avec succès.

Dans les pages précitées, vous reconnaissez également plusieurs éléments positifs liés à la culture de performance qui caractérise notre direction, culture dont l'origine est en partie à trouver dans les exigences posées dans le cadre de la mise en œuvre de la Loi fédérale sur l'assurance chômage (LACI).

Enfin, tout en partageant votre analyse pour ce qui a trait à la mise en place d'une vision d'ensemble de notre portefeuille des risques et de sa gestion, nous relevons comme vous qu'outre la CCh, tant la Direction de l'autorité cantonale de l'emploi (DIACE) que la Direction de l'insertion professionnelle et du placement (DIPP) ont mené des démarches abouties, bien que partiellement actualisées, de gestion des risques. Elles témoignent d'une préoccupation préexistante pour la gestion des risques au sein de la direction.

Direction générale de l'emploi et du marché du travail – DGEM
Département de l'économie, de l'innovation, de l'emploi et du patrimoine – DEIEP
www.vd.ch/emploi – T + 41 21 316 61 04 – info.dgem@vd.ch

Au-delà de cette précision, la DGEM n'a pas de remarque ou commentaire particulier à formuler à la lecture de votre rapport.

En conclusion, nous souhaitons profiter de ces lignes pour saluer la qualité de nos échanges et relever la richesse et l'intérêt de l'approche défendue dans votre rapport.

Je vous prie de bien vouloir agréer, Monsieur le Vice-Président, mes salutations distinguées.

Françoise Favre

Directrice générale

Direction générale de l'emploi et du marché du travail – DGEM
Département de l'économie, de l'innovation, de l'emploi et du patrimoine – DEIEP
www.vd.ch/emploi – T + 41 21 316 61 04 – info.dgem@vd.ch

canton de vaud

Direction générale de l'enseignement postobligatoire

Rue Saint-Martin 26
1014 Lausanne

Cour des comptes
M. Guy-Philippe Bolay
Magistrat
Rue de Langallerie 11
1014 Lausanne

Réf. : LEN/PCO

Lausanne, le 21 novembre 2023

Consultation du projet de rapport sur l'audit de la gestion intégrée des risques

Monsieur le Magistrat, Cher Monsieur,

Dans le cadre de la consultation citée en titre, nous avons l'avantage de vous transmettre la prise de position de la DGEP sur le projet de rapport cité en titre.

Nous tenons à vous remercier d'avoir adopté une approche non stigmatisante et résolument orientée sur la recherche d'une solution harmonisée à l'échelle de l'ensemble de l'Etat de Vaud, au-delà des six services retenus pour votre audit. Nous vous remercions également d'avoir intégré les remarques que nous vous avons transmises le 20 octobre 2023. Nous saisissons également cette occasion pour relever le cadre rigoureux et respectueux dans lequel l'audit de la Cour des comptes s'est résolument inscrit.

De manière générale, la DGEP souscrit aux constats et conclusions présentées dans le rapport, notamment sur l'importance de prendre des mesures adéquates et pondérées qui visent à éviter ou à atténuer les risques auxquels l'Etat de Vaud et ses services sont par définition soumis. Bien que largement disposés à déployer une méthode aussi proportionnée que possible, nous attirons l'attention de la Cour des comptes sur le fait que la mise en œuvre d'un système intégré tel que préconisé nécessitera des moyens supplémentaires appropriés et en suffisance, quand bien même nous nous employons d'ores et déjà à minimiser les principaux risques que nous avons identifiés depuis plus de cinq ans désormais. Sous réserve de la position du Conseil d'État, la DGEP est donc prête à aller dans le sens des préconisations émises.

En ce qui concerne les points plus précis du projet de rapport, nous soutenons toutefois qu'au chapitre relatif aux fonctions, rôles et responsabilités (pp. 39 à 41) les directeurs généraux devraient assurer la responsabilité de l'application du système de gestion intégrée des risques qui sera retenu et des mesures visant à éviter ou à atténuer les risques. En effet, « assumer la responsabilité des risques » (p. 40) en tant que telle nous paraît invraisemblable puisqu'elle dépend souvent d'autres Services de support de l'ACV et de plusieurs facteurs exogènes.

Département de l'enseignement et de la formation professionnelle
Direction générale de l'enseignement postobligatoire (DGEP)
www.vd.ch/dgep – T 021 316 63 04 – info.dgep@vd.ch

Personne de contact : Pedro Coelho

En vous remerciant une nouvelle fois pour l'approche adoptée dans cet audit ainsi que pour les recommandations qui permettront sans aucun doute de mieux maîtriser les risques, je vous adresse, Monsieur le Magistrat, cher Monsieur, mes salutations les plus cordiales.

Lionel Eperon

Directeur général

Annexe mentionnée

Copie

- Mme Fanny Spichiger, Secrétaire générale du DEF

Département de l'enseignement et de la formation professionnelle
Direction générale de l'enseignement postobligatoire (DGEP)
www.vd.ch/dgep – T 021 316 63 04 – info.dgep@vd.ch

Personne de contact : Pedro Coelho

Département des institutions, du territoire et du sport

Le Secrétaire général

Place du Château 1
1014 Lausanne

Cour des comptes
A l'att. de Madame la Présidente Valérie Schwaar et Monsieur le Vice-Président Guy-Philippe Bolay
Rue de Langallerie 11
1014 Lausanne

Lausanne, le 23 novembre 2023

Projet de rapport d'audit de la gestion intégrée des risques

Madame la Présidente,
Monsieur le Vice-Président,

Je me réfère à votre envoi du 2 novembre 2023. Votre projet de rapport d'audit mentionné en titre m'est bien parvenu et j'en ai pris connaissance avec intérêt.

En premier lieu, je tiens à vous remercier de m'avoir donné la possibilité de m'exprimer concernant cet objet et salue le travail important effectué par votre autorité. De plus, je souhaite soulever l'excellent climat dans lequel l'audit s'est déroulé ainsi que la disponibilité des personnes représentant la Cour des comptes.

Sur le fond de l'audit, je partage les constats qui ont été faits, notamment en ce qui concerne l'absence d'une stratégie définissant la gestion intégrée des risques (GDR) au sein de l'Administration cantonale vaudoise (ACV).

Toutefois, les missions diverses et variées des services de l'ACV rendent complexes la mise en place d'une approche homogène de GDR. La mise en œuvre doit être adaptée aux entités, rester simple, sans être lourde sur le plan administratif.

Aussi, j'ai pris bonne note que l'utilisation du modèle COSO n'est pas obligatoire et que l'ACV peut adopter, selon ses besoins, d'autres modèles de GDR.

A cet égard, et après examen du projet de rapport, je vous informe que le Secrétariat général du Département des institutions, du territoire et du sport n'a pas de remarque particulière à formuler.

En vous remerciant de l'attention portée à la présente, je vous présente, Madame la Présidente, Monsieur le Vice-Président, mes meilleures salutations.

Stéphane Wicht
Secrétaire général

www.vd.ch – Tél. : + 41 21 316 45 15
info.sgdits@vd.ch

canton de vaud

Le Chancelier a.i.

Château cantonal
1014 Lausanne

Cour des comptes
Monsieur le Vice-Président
Guy-Philippe Bolay
Rue de Langallerie 11
1014 Lausanne

Lausanne, le 24 novembre 2023

Audit de la gestion intégrée des risques- détermination de la Chancellerie d'Etat sur la base du projet de rapport de la Cour des comptes

Monsieur le Vice-Président,
Cher Monsieur,

La Chancellerie vous remercie pour la transmission du projet de rapport de la Cour des comptes portant sur l'audit de la gestion intégrée des risques et se détermine comme suit, en tant qu'entité auditée dans le cadre de la consultation officielle sur ce document, conformément à l'art. 17 RLCComptes.

La Chancellerie d'Etat, en vertu de son positionnement en soutien aux activités du Conseil d'Etat remplit de nombreuses missions de coordination, qu'elle exerce de manière transversale, lui offrant ainsi une vision assez large sur les risques qui pourraient affecter l'Administration cantonale vaudoise (ACV).

Si l'on peut relever l'absence de système formalisé de gestion des risques, à l'échelon de la Chancellerie ou à celui de l'Etat, il convient en revanche de mettre en évidence quelques éléments, dans ses missions légales comme dans ses opérations, qui contribuent à limiter fortement les risques pesant tant sur le service que sur les activités du gouvernement et de l'ACV.

- Les activités de coordination menées, par exemple au travers de l'activité du collège des secrétaires généraux (CSG), contribuent à écarter les problèmes formels, à vérifier le respect des procédures et règles existantes en amont des décisions du Conseil d'Etat, afin que le collège gouvernemental puisse exercer sa fonction politique dans les meilleures conditions, ces risques écartés.

- Dans sa mission de garantie de l'exactitude des décisions du Conseil d'Etat, la Chancellerie contribue également à la sécurisation des éléments produits par le Conseil d'Etat ; décisions, textes ou communications. Il s'agit également là d'une gestion des risques qui s'exerce au quotidien.

Chancellerie d'Etat
www.vd.ch – T 41 21 316 41 59
info.chancellerie@vd.ch

canton de vaud

Le Chancelier a.i.
Audit de la gestion intégrée des risques- détermination de la Chancellerie d'Etat sur la base du projet de rapport de la Cour des comptes

- De même, les risques de communication sont au cœur de l'activité du BIC (Bureau de communication de l'Etat de Vaud, entité de la Chancellerie) et de l'ensemble de la fonction dédiée à la communication dans les départements et les services, qui opèrent dans le cadre de la politique de communication voulue par le CE et coordonnée par le BIC.

- Il convient de relever également que la prise en considération des risques et des incertitudes sur le plan financier et économique est pratiquée dans le cadre de toute proposition soumise au Conseil d'Etat, au même titre que les conséquences sur le personnel, les impacts sur le climat et la durabilité notamment.

- Enfin, en tant que service, la Chancellerie assume également ses responsabilités en termes de santé et sécurité au travail et se préoccupe des risques liés aux ressources humaines à disposition des missions qu'elle remplit.

En ce qui concerne les risques majeurs pesant sur la population vaudoise dans le domaine des dangers naturels, techniques et sociétaux, il convient de rappeler qu'ils ont fait l'objet d'une analyse mise à jour par le Conseil d'Etat en 2022, sur la base des travaux menés par le Service de la sécurité civile et militaire (SSCM), selon les recommandations et méthodologies fédérales en la matière.

Ainsi, et même en l'absence d'une démarche formalisée, standardisée et généralisée, une attention constante et centrale est portée par le Conseil d'Etat, la Chancellerie ainsi que les départements et les services afin que les actions, projets et prestations définies puissent se développer dans le cadre le plus prévisible et sécurisé possible.

Vous sachant gré d'avoir consulté la Chancellerie et vous remerciant à nouveau de l'attention que vous porterez à cette détermination, nous vous prions de croire, Monsieur le Vice-Président, Cher Monsieur, à l'assurance de notre considération distinguée.

Le Chancelier a.i.

François Vodoz

6. Annexes

Annexe I — Liste des principales abréviations utilisées

ACV	Administration cantonale vaudoise
BCM	Business Continuity Management (plan de continuité d'activité)
BIC	Bureau d'information et de communication de l'Etat
CCF	Contrôle cantonal des finances
CE	Conseil d'Etat
CO	Code des obligations
COFIN	Commission des finances du Grand Conseil vaudois
COGES	Commission de gestion du Grand Conseil vaudois
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSG	Collège des secrétaires généraux
DGEM	Direction générale de l'emploi et du marché du travail
DGEP	Direction générale de l'enseignement postobligatoire
DGIP	Direction générale des immeubles et du patrimoine
DGNSI	Direction générale du numérique et des systèmes d'information
DGRH	Direction générale des ressources humaines
EMPD	Exposé des motifs et projet de décret
ERM	Enterprise Risk Management (*gestion des risques* d'entreprise)
GDR	*Gestion des risques*
INTOSAI	*International Organisation of Supreme Audit Institutions* (Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques)
IRGC	*International Risk Governance Council* (Conseil international de la gouvernance des risques)
ISSAI	*International Standards of Supreme Audit Institutions* (Normes internationales faisant autorité en matière d'audit du secteur public)
ISO	*International Standardization Organization* (Organisation internationale de normalisation)
LCComptes	Loi sur la Cour des comptes du 12 mars 2013
LFin	Loi sur les finances
LOCE	Loi sur l'organisation du Conseil d'Etat
NAS	Normes d'audit suisses
PCE	Proposition au Conseil d'Etat
RH	Ressources humaines
SAGEFI	Service d'analyse et de gestion financière
SAN	Service des automobiles et de la navigation
SCI	Système de contrôle interne
SECO	Secrétariat d'Etat à l'économie
SG-DITS	Secrétariat général du Département des institutions, du territoire et du sport
SIEL	Système d'information de l'exécutif et du législatif
SPEN	Service pénitentiaire

Annexe II — Glossaire

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	Créé 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.
COSO I et COSO II	Le référentiel initial, appelé COSO I et datant de 1992, traitait du contrôle interne. Depuis 2002, ce modèle a évolué vers un second corpus dénommé COSO II qui concerne la *gestion des risques* d'entreprise. Une deuxième mise à jour date de 2017 : voir *COSO-ERM 2017*.
COSO-ERM 2017	Le document de référence en vigueur actuellement est « Le management des risques d'entreprise – Une démarche intégrée à la stratégie et à la performance ». Il résulte d'une mise à jour du cadre COSO en 2017, pour tenir compte de l'évolution de la complexité des risques, de l'émergence de nouveaux risques et de la demande d'un reporting de plus en plus développé de la part des conseils et des dirigeants.
Gestion des risques[33]	La gestion du risque est 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. Elle fait partie intégrante des mécanismes d'une saine gestion. Il ne s'agit pas nécessairement d'éviter le risque en cas de menaces éventuelles.
Gestion intégrée des risques[34]	La gestion du risque ne peut être efficace si elle est cloisonnée. Ainsi, la gestion intégrée du risque favorise 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. Elle favorise la prise de décisions stratégiques qui contribuent à l'atteinte des objectifs globaux de l'organisation. La gestion intégrée du risque exige une évaluation continue des risques auxquels une organisation peut faire face à tous les niveaux, le regroupement des résultats à l'échelle de l'organisation et une communication, une surveillance et un examen adéquats. Les résultats regroupés servent alors à donner fond aux décisions et aux pratiques de l'organisation.
International Risk Governance Council	L'*International Risk Governance Council (IRGC)* est une fondation indépendante à but non lucratif basée en Suisse, dont la mission est d'améliorer la *gestion des risques* émergents et systémiques qui ont ou pourraient avoir un impact sur la santé humaine et environnementale, l'économie et la société, et la durabilité globale. Jusqu'au 31 juillet 2023, ses activités étaient organisées par l'*International Risk Governance Center* de l'EPFL.
ISO 9001	Norme de l'ISO : Management de la qualité
ISO 31000	Norme de l'ISO : Management du risque

[33] Extrait du Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, mai 2016
[34] Idem

Propriétaire d'un risque[35]	Personne ayant le pouvoir (par le biais de sa position hiérarchique ou fonctionnelle, de ses compétences ou des ressources à sa disposition) de maintenir un risque sous contrôle, de coordonner la mise en place des plans d'action ou le maintien des contrôles et en général de le gérer selon la stratégie de traitement choisie et validée. La personne propriétaire d'un risque est en dernière instance déterminée par l'autorité décisionnelle ; le choix est indépendant de la gravité du risque, et ne dépend que du pouvoir d'intervention sur le risque et de sa pertinence pour une entité ; l'autorité décisionnelle peut décider de cumuler ce rôle ou de le déléguer de manière appropriée.
Risque	Le risque est l'effet de l'incertitude sur l'atteinte des objectifs. Pour chaque risque considéré, il faut évaluer deux choses : la probabilité ou l'éventualité que l'événement survienne et l'ampleur de ses répercussions ou de ses conséquences s'il survient. Il faut rappeler qu'étant donné que le risque se rapporte à l'effet de l'incertitude, et donc à une perspective d'avenir, les risques se distinguent des enjeux, des problèmes ou des conditions existants, pour lesquels la probabilité qu'ils surviennent ne serait pas en cause.[36] On peut distinguer[37] : - les risques **externes ou exogènes**, parmi lesquels on peut trouver ceux liés à la société en général et ceux liés à la branche ou au secteur économique ; - les risques **internes ou endogènes**, classés en trois catégories : stratégiques, opérationnels et financiers.
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.
Système de contrôle interne	Selon la directive d'exécution n° 22 du SAGEFI, le système de contrôle interne (SCI) englobe toutes les méthodes, les procédures et les mesures organisationnelles mises en place par la direction d'une entité afin de fournir un travail efficace qui minimise les risques et évite les erreurs dans les états financiers. La direction et le personnel, à tous les niveaux, doivent être impliqués dans ce processus. Selon la NAS-890, une entreprise devrait disposer d'un SCI opérationnel en permanence dans tous les domaines de son activité. Toutefois, l'organe de révision n'est tenu d'en vérifier et confirmer l'existence que dans l'optique du rapport financier. Ce contrôle ne porte donc pas sur l'efficacité et l'efficience du SCI.
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.

[35] Extrait du Manuel méthodologique de gestion des risques, Etat de Genève, version 2.0 – 18 décembre 2015

[36] Extrait du Guide de gestion intégrée du risque, Secrétariat du Conseil du Trésor du Canada, mai 2016

[37] Portail PME, Administration fédérale, https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/finances/gestion-risques/planification-risques/identification-risque.html

Annexe III – L'audit réalisé

La Cour des comptes 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 sa « Charte éthique et son Code de déontologie ». L'audit a été réalisé conformément aux normes internationales sur les audits de performance établies par l'Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques (INTOSAI).

La Cour s'est notamment 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*. Cette norme INTOSAI est actuellement en révision, en raison de l'évolution du cadre COSO.

L'équipe d'audit était composée de Monsieur Guy-Philippe Bolay, magistrat responsable, de Madame Patricia Girardbille, cheffe de mandat d'audit en charge, et Monsieur Fabrice Berset, chef de mandat en soutien. Elle a été appuyée par une experte spécialisée en GDR et en conseils aux administrations publiques.

La collecte et l'analyse des informations probantes

Les éléments probants suffisants et adéquats pour fonder raisonnablement les conclusions du rapport ont principalement été établis au moyen des procédures suivantes :

- **Entretiens ciblés avec la direction des six entités auditées** – L'équipe d'audit a consacré deux demi-journées dans chacune des entités auditées à interviewer les membres de la direction pour compléter le questionnaire couvrant chacune des cinq composantes du modèle *COSO-ERM 2017*. Les données obtenues ont été compilées et comparées de manière à obtenir une vision transversale de la GDR au sein des entités auditées, afin de pouvoir faire l'état des lieux souhaité et dégager des recommandations de portée générale.
- **Analyse de documents** — Afin d'étayer les réponses reçues et de compléter les informations transmises lors des entretiens, la Cour a examiné différents documents liés à l'organisation, aux processus de travail et à la gestion de l'activité des six entités auditées, notamment des procédures et directives de travail internes, des organigrammes et cahiers des charges, des procès-verbaux de séance, etc.
- **Analyse des résultats obtenus** – Sur la base des réponses au questionnaire et des documents probants reçus, chacune des cinq composantes du modèle COSO a été évaluée sur une échelle de 1 à 5 permettant d'estimer son degré de maturité. Les notations obtenues fournissent un indice du degré de maturité de l'évaluation de la GDR dans les entités auditées. Les données obtenues ont été compilées et comparées de manière à obtenir une vision transversale de la GDR au sein des services audités.
- **Entretiens avec le CCF et le SAGEFI** – Un entretien a eu lieu avec la direction du SAGEFI pour connaître le soutien apporté aux services pour la mise en place du SCI financier. L'équipe d'audit s'est aussi entretenue avec la direction du CCF pour obtenir des détails sur les procédures menées pour certifier le SCI financier des entités auditées et a consulté les rapports émis par le CCF.

Les textes-cadres

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.
- Guide de la gestion intégrée des risques du Secrétariat du Conseil du Trésor du Canada mai 2016 : https://www.canada.ca/fr/secretariat-conseil-tresor/organisation/gestion-risque/guide-gestion-integree-risque.html#toc2_1
- Manuel de *gestion des risques* de la Confédération, version du 22 mars 2022
- Rapports du Contrôle fédéral des finances : en particulier « Audit de la *gestion des risques* de la Confédération en tant qu'instrument de pilotage » (rapport n° EFK-17476 du 3 mai 2018)
- Politique de *gestion des risques* de l'Etat de Genève — Législature 2018-2023, Adoptée par le Conseil d'Etat le 10 avril 2019
- Directive transversale sur la *gestion des risques* de l'Etat de Genève, approuvée le 10 décembre 2015
- Manuel de *gestion des risques* de l'Etat de Genève, version 2.0 du 18 décembre 2015
- Guide rapide sur la *gestion des risques* opérationnels de l'Etat de Genève, version 2.0 du 18 décembre 2015
- Directives sur la *gestion des risques* du Canton de Berne, approuvées le 24 novembre 2021

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. 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.

Annexe IV — Cadre légal

Cour des comptes VD

- Art. 4 al. 1 let. b LCComptes : la vérification de l'évaluation de la *gestion des risques* des entités soumises à son champ de contrôle est une des attributions de la Cour des comptes.
- Art. 15 al. 2 RCComptes : l'audit de la vérification de l'évaluation de la *gestion des risques* est l'un des deux types d'audit que la Cour des comptes conduit selon sa méthodologie.

Secteur public — Canton de Vaud

Seuls les risques au niveau financier sont traités dans la réglementation vaudoise :

- Art 15 al 2 let i LFin : le département en charge des finances de l'Etat a notamment la compétence d'évaluer les risques financiers.
- Directive d'exécution n° 22 du SAGEFI sur le *système de contrôle interne* (rendue obligatoire pour tous les services de l'administration par l'art. 16 al. 1 let e LFin) : définit le contrôle interne comme permettant de minimiser les risques et éviter les erreurs dans les états financiers. Les services doivent notamment développer des processus adéquats pour identifier, apprécier et surveiller les risques encourus.

Secteur public — Confédération

L'Ordonnance sur les finances de la Confédération (art. 50 OFC) stipule que les départements et la Chancellerie fédérale gèrent les risques dans leur domaine de compétence selon les directives du Conseil fédéral.

La 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 constitue un des documents fondateurs.

Les Directives du Conseil fédéral du 24 septembre 2010 sur la politique de *gestion des risques* menée par la Confédération fixent le cadre d'une GDR intégrée applicable à l'entier des départements et unités administratives de la Confédération (définition, champ d'application, buts, principes et rôles et responsabilités). La GDR en tant qu'instrument de conduite fait partie intégrante du processus de travail et de conduite.

Les Directives de l'AFF du 21 novembre 2011 sur la *gestion des risques* menée par la Confédération concrétisent les directives du Conseil fédéral en définissant des règles uniformes pour la mise en œuvre du processus de GDR (version du 31 mars 2016).

Secteur privé — Code des obligations (CO)

Selon l'art 961 c CO, les exigences en matière de présentation des comptes applicables aux grandes entreprises (soumises au contrôle ordinaire, soit les sociétés ouvertes au public et les sociétés qui dépassent les valeurs de l'art 727 al 1 ch2 CO) leur imposent de rédiger un rapport annuel qui précise notamment la réalisation d'une évaluation des risques.

Annexe V — Normes applicables (liste non exhaustive)

COSO

COSO-ERM 2017 – Le management des risques de l'entreprise — Une démarche intégrée à la stratégie et à la performance

Cette norme est reconnue au niveau international et permet de dériver des critères d'audit afin d'évaluer un système de *gestion des risques* intégré. Voir le glossaire pour plus d'informations.

Voir le document de référence : Le management des risques de l'entreprise, Une démarche intégrée à la stratégie et à la performance, Synthèse, COSO, Traduit de l'anglais, juin 2017 (https://www.ifaci.com/wp-content/uploads/COSO-ERM-2017_synthe%CC%80se.pdf)

INTOSAI

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, notamment :

INTOSAI GOV 9100 (2004, en révision) — Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public.

INTOSAI GOV 9130 (2004, en révision) — Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public – informations complémentaires sur la *gestion des risques* des entités.

ISO — Organisation internationale de normalisation

ISO 31000:2018 Management du risque — Lignes directrices

Cette norme fournit des lignes directrices et des principes généraux pour l'identification, l'évaluation, le traitement et le suivi des risques dans toutes les organisations, qu'elles soient du secteur public, privé ou à but non lucratif. L'*ISO 31000:2018* n'a pas vocation à servir de base à une certification et ne fournit pas de méthodologie spécifique pour la GDR, mais plutôt des bonnes pratiques à suivre.

La norme encourage une approche systématique, proactive et continue de la GDR, en intégrant celle-ci dans les processus de prise de décision et de gestion de l'organisation. Elle souligne également l'importance de la communication et de la consultation régulières avec les parties prenantes concernées.

Les principes clés incluent l'évaluation continue des risques, la prise en compte du contexte organisationnel, l'identification des parties prenantes, l'établissement de critères de risque, l'adaptation des stratégies de traitement des risques et la promotion d'une culture de GDR. Ces principes visent à améliorer la performance, à renforcer la résilience et à soutenir la réalisation des objectifs stratégiques de l'organisation.

Les normes ISO étant réexaminées tous les cinq ans, l'*ISO 31000:2018* est en cours d'examen.

ISO 31073:2022 Management du risque — Vocabulaire

Ce document définit des termes génériques relatifs au management des risques auxquels font face les organismes.

ÖNORM

L'Austrian Standards Institute (anciennement : Österreichisches Normungsinstitut) est un organisme de normalisation, membre de l'ISO pour l'Autriche. Il a publié la norme ÖNORM D 4901 [38] (anciennement ONR 49001[39]), qui est basée sur la norme *ISO 31000* et représente sa mise en œuvre dans la pratique.

Cette norme est citée ici, car c'est l'un des systèmes normatifs usuels (avec *ISO 31000*) sur lesquels s'appuient les directives et le Manuel de *gestion des risques* de la Confédération.

ÖNORM D 4901

Cette norme décrit les éléments généralement applicables d'un système de GDR. Le processus de *gestion des risques* en fait partie. Les caractéristiques des différents éléments du système et du processus dépendent de la taille de l'organisation, de son exposition aux risques, de la complexité des processus et de l'évolution de son environnement. Il est recommandé de définir et de documenter les éléments du système et du processus de GDR de manière à pouvoir les démontrer et les vérifier de façon objective. Il est ainsi possible de déterminer si une organisation dispose d'un système de GDR approprié. Le système de GDR peut être intégré dans les systèmes de gestion existants ou introduit et mis en œuvre en tant que système distinct.[40]

[38] ÖNORM D 4901 : Management du risque pour les organisations et les systèmes — exigences pour le système de management du risque – guide pour la mise en œuvre de l'ISO 31000.
[39] Österreichisches Normungsinstitut, ONR 49000:2010, management du risque pour organismes et systèmes (2010)
[40] Source : traduit de https://shop.austrian-standards.at/action/en/public/details/687870/OENORM_D_4901_2021_01_01

Annexe VI — Questionnaire

A. Gouvernance et culture

Principes	Description des principes	Questions principales
A. 1. Exercer une surveillance des risques	Le Conseil d'Etat assure la surveillance de la mise en œuvre du programme de législature et assume les responsabilités en matière de gouvernance pour soutenir la direction du service dans la réalisation de leur stratégie et des objectifs opérationnels. Il met en place les conditions-cadres permettant aux départements et aux services d'élaborer leur stratégie, leurs objectifs et d'évaluer les risques et opportunités.	***Questions pour tous :*** Du point de vue de votre service, comment évaluez-vous les conditions-cadres mises en place au sein de l'Etat pour s'assurer qu'il atteint les objectifs fixés et prendre en compte ses risques et leurs conséquences ? ***Question supplémentaire pour les services :*** Comment, au sein de votre service, vous assurez-vous d'atteindre les objectifs fixés et de prendre en compte vos risques et leurs conséquences ? ***Question supplémentaire pour le SG :*** Comment vous assurez-vous que les services de votre département atteignent les résultats attendus et comment tenez-vous compte des risques et de leurs conséquences? ***Question supplémentaire pour la Chancellerie :*** Quelle mission le Conseil d'Etat vous donne-t-il pour s'assurer de la mise en œuvre coordonnée et cohérente des objectifs opérationnels, pour vérifier la mise en œuvre du programme de législature et surveiller les risques ?
		Qui porte la responsabilité de la surveillance des risques au sein du service et comment est-elle exercée ?
A. 2. Définir les structures organisationnelles	L'entité définit des structures organisationnelles dans la perspective de la réalisation de la stratégie et des objectifs opérationnels.	Pourriez-vous nous décrire la structure organisationnelle de votre service ?
		Comment définissez-vous les rôles et responsabilités de chacun et les éventuelles délégations de pouvoirs ? Comment gérez-vous les droits d'accès aux systèmes et aux locaux ?
A. 3. Définir la culture souhaitée	L'entité définit les comportements attendus qui caractérisent la culture souhaitée par l'entité.	Comment décririez-vous la culture du risque au sein de votre service ?
A. 4. Démontrer l'engagement en faveur des valeurs fondamentales	L'entité démontre son engagement pour les valeurs fondamentales de l'entité.	Comment définiriez-vous le degré d'intégrité et les valeurs éthiques au sein de votre service ?
A. 5. Attirer, former et fidéliser des personnes compétentes	L'entité s'engage à développer le capital humain en adéquation avec la stratégie et les objectifs opérationnels.	Comment évalueriez-vous votre service du point de vue de la politique des ressources humaines ?

B. Stratégie et définition des objectifs

Principes	Description des principes	Questions principales (à poser aux audités)
B. 6. Analyser le contexte de l'organisation	L'entité prend en considération l'impact potentiel de son contexte sur le profil de risque.	Comment identifiez-vous et mesurez-vous les éléments susceptibles d'impacter votre activité et son développement au cours des prochaines années ?
B. 7. Définir l'appétence pour le risque	L'entité définit l'appétence pour le risque dans le contexte de la création, de la préservation et de la concrétisation de la valeur.	Comment définiriez-vous la marge de manœuvre et l'attitude de votre service par rapport aux risques ? (appétence et tolérance au risque) *Définitions - 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.*
B. 8. Évaluer les stratégies alternatives	L'entité définit sa stratégie pour atteindre ses objectifs. Elle envisage des stratégies alternatives et leurs impacts potentiels sur le profil de risque.	Avez-vous défini une stratégie pour le service, un plan d'action pour assurer le développement et la cohérence de ses prestations ? Si oui, comment a-t-elle été définie ? Si non, comment vous assurez-vous du développement et de la cohérence de vos prestations ?
B. 9. Définir les objectifs opérationnels	L'entité prend en considération les risques lors de la définition, à différents niveaux, d'objectifs opérationnels qui soient en phase avec la stratégie et la soutiennent.	Comment les objectifs opérationnels sont-ils définis ?

C. Performance

Principes	Description des principes	Questions principales (à poser aux audités)
C. 10. Identifier les risques	L'entité identifie les risques qui affectent la réalisation de la stratégie et des objectifs opérationnels.	Comment identifiez-vous les évènements (risques) pouvant affecter la réalisation de votre stratégie et de vos objectifs ?
C. 11. Évaluer la criticité des risques	L'entité évalue la criticité des risques.	Comment évaluez-vous la criticité (probabilité et impact) des risques ?
C. 12. Prioriser les risques	L'entité priorise les risques pour sélectionner les modalités de traitement de ces risques.	Comment les risques sont-ils priorisés pour définir les modalités de traitement ?
C. 13. Mettre en œuvre les modalités de traitement des risques	L'entité identifie et sélectionne les modalités de traitement des risques.	Comment identifiez-vous et sélectionnez-vous les modalités de traitement des risques ?
C. 14. Développer une vision globale du portefeuille de risques	L'entité développe une vision globale et une évaluation du portefeuille de risques.	Avez-vous développé une vision globale de votre portefeuille de risques ?

D. Revue et actualisation

Principes	Description des principes	Questions principales (à poser aux audités)
D. 15. Évaluer les changements substantiels *(concentré sur ce qui est nouveau)*	L'entité identifie et évalue les changements qui pourraient affecter substantiellement la stratégie et les objectifs opérationnels.	Comment identifiez-vous les changements dans les éléments susceptibles d'impacter votre activité et son développement au cours des prochaines années ?
D. 16. Réexaminer les risques et la performance *(réexamen de l'actuel, concentré sur le risque résiduel)*	L'entité revoit la performance de ses activités et prend en considération les risques.	Comment est réalisée la mise à jour des processus de gestion des risques ? Comment le risque résiduel est-il suivi ?
D. 17. Poursuivre l'amélioration du management des risques de l'organisation	L'entité poursuit l'amélioration du management des risques de l'organisation.	Avez-vous introduit un processus d'amélioration continue du management des risques au sein de l'organisation ?

E. Information, communication et reporting

Principes	Description des principes	Questions principales (à poser aux audités)
E. 18. Tirer parti des données et des technologies	L'entité exploite les systèmes d'information et technologiques de l'entité pour soutenir le management des risques de l'organisation.	Quels sont les moyens de communication utilisés pour la gestion des risques ? Les outils et technologies à disposition sont-elles utilisées à leur plein potentiel ?
E. 19. Communiquer les informations relatives aux risques *(à l'interne)*	L'entité utilise les moyens de communication pour soutenir le management des risques de l'organisation.	Quelle est la communication à propos de la gestion des risques à l'interne de l'organisation ?
E. 20. Rendre compte des risques, de la culture et de la performance *(à l'externe)*	L'entité rend compte des risques, de la culture et de la performance à différents niveaux et dans toute l'entité.	Quelle est la communication aux différentes parties prenantes à propos de la gestion des risques ?

Annexe VII —Modèle de maturité

A. Gouvernance et culture						
Principes	**Critères d'évaluation**	***Peu fiable*** ***N'existe pas ou non appliqué*** ***1***	***Informel*** ***Existe mais n'est pas documenté*** ***2***	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	***Evalué*** ***Existe de manière développée et documentée*** ***4***	***Intégré*** ***Existe de manière optimisée (stratégie et performance)*** ***5***
A. 1. Exercer une surveillance des risques	Des conditions-cadres sont mises en place au sein de l'Etat de manière à s'assurer qu'il atteint les objectifs fixés, en évaluant les risques et ses conséquences. L'Etat promeut la gestion des risques et organise la surveillance de l'évaluation des risques.	*Les conditions-cadres au sein de l'Etat ne permettent pas de vérifier l'atteinte des objectifs ni de gérer leurs risques.*	*L'Etat n'a pas établi formellement des conditions-cadres pour vérifier l'atteinte de ses résultats et la gestion de ses risques mais il promeut auprès de ses services l'importance de la gestion des risques lors des discussions stratégiques.*	*L'Etat a défini formellement, mais de manière succincte, des conditions-cadres pour vérifier l'atteinte de ses résultats et s'assurer de la gestion de ses risques par une surveillance adéquate.*	*L'Etat a défini formellement des conditions-cadres pour la gestion de ses risques et s'assurer de leur surveillance. Il évalue au moyen d'indicateurs l'atteinte de ses objectifs et les conséquences en termes de risques.*	*L'Etat élabore sa stratégie et vérifie l'atteinte de ses objectifs sur la base d'une gestion intégrée des risques, déclinée dans tous ses services.*
	La surveillance exercée sur les risques est adéquate car elle est : - indépendante (pas de conflits d'intérêt ou de loyauté) ; - compétente (connaissances techniques et expérience suffisantes) ; - suffisante (en temps et en moyens, degré d'implication).	*La surveillance n'est ni indépendante, ni compétente, ni suffisante.*	*La surveillance est faible, car deux des trois critères ne sont pas respectés.*	*Une surveillance de base est exercée, 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 au plus haut niveau de l'Etat.*
A. 2. Définir les structures organisationnelles	La structure et l'organisation de l'entité sont clairement définies et documentées, adaptées à sa taille et à la complexité de ses tâches. Un organigramme détaillé du service existe, il est à jour et correspond à l'organisation effective. L'organisation a été réfléchie de manière à clarifier les processus décisionnels et faciliter les flux d'information et de communication.	*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 stratégie et la politique de risques de l'organisation.*
	Les rôles et responsabilités dans l'organisation et les délégations de pouvoir sont définis formellement, en particulier en lien avec la gestion des risques, et sont connus de l'ensemble des collaborateurs.	*Les rôles, les responsabilités et les délégation des pouvoirs - ne sont pas clairs dans l'organisation.*	*Les rôles et responsabilités et les délégations de pouvoir sont clairs mais ils ne sont pas formalisés. Ils ne sont pas nécessairement connus de l'ensemble des collaborateurs.*	*Les rôles et responsabilités et les délégations de pouvoir sont formalisés et connus de l'ensemble des collaborateurs.*	*Les rôles et responsabilités et les délégations de pouvoir sont formalisés et connus 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.*	*Les rôles et responsabilités et les délégations de pouvoir sont formalisés. Ils sont connus de l'ensemble des collaborateurs et font partie de la stratégie de l'organisation, notamment au niveau de l'optimisation de sa politique des risques.*
	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.*

Principes	Critères d'évaluation	*Peu fiable* *N'existe pas ou non appliqué* *1*	*Informel* *Existe mais n'est pas documenté* *2*	*Standard* *Existe de manière basique et documentée* *3 (norme attendue)*	*Evalué* *Existe de manière développée et documentée* *4*	*Intégré* *Existe de manière optimisée (stratégie et performance)* *5*
A. 3. Définir la culture souhaitée	Les principes de gestion des risques de l'entité sont communiqués : - une politique interne écrite spécifique à la gestion des risques de l'entité existe ; - les principes de gestion des risques de l'entité sont évoqués ou rappelés dans d'autres politiques internes ; - le personnel est informé par d'autres biais (ex : formation) ; - 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.*
	L'ensemble du personnel adhère aux politiques et aux 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 (adhésion par silo).*	*En général, une adhésion moyenne au travers de l'organisation. Quelques déviations persistent.*	*Valeurs collectives intégrées, adhésion forte aux politiques, procédures transverses.*
	La direction adopte une attitude favorable au bon fonctionnement du système de gestion des risques mis en place (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, voire hostile.*	*Support passif, manque d'indépendance ou de compétence technique.*	*Fait de la promotion dans son silo et supporte le concept.*	*Fait de la promotion et encourage l'action dans toute l'organisation.*	*Est un acteur "champion" avec une forte compréhension du système.*
	Les cadres et le personnel de l'organisation sont convaincus de 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.*
	L'ensemble de l'organisation est vigilant par rapport aux risques.	*Aucune vigilance dans l'ensemble de l'organisation.*	*Seuls quelques employés ou quelques entités sont vigilants aux risques. Pas de langage commun à l'échelle de l'organisation.*	*Un langage 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.*
	L'organisation fait partie de commissions intercantonales ou de groupements professionnels et respecte les normes édictées par ces entités.	*L'organisation ne fait pas partie de commissions intercantonales ou de groupements professionnels, ne respecte pas ses normes et n'utilise pas ses prestations.*	*L'organisation ne fait pas partie de commissions intercantonales ou de groupements professionnels mais applique en partie ses normes ou utilise occasionnellement ses prestations.*	*L'organisation est membre de commissions intercantonales ou de groupements professionnels, respecte ses normes et utilise occasionnellement ses prestations.*	*L'organisation est membre de commissions intercantonales ou de groupements professionnels et les normes sont intégrées à la gestion de l'organisation.*	*L'organisation est membre actif de commissions intercantonales ou de groupements professionnels et les normes professionnelles influencent les objectifs stratégiques de l'organisation.*
A. 4. Démontrer l'engagement en faveur des valeurs fondamentales	Les valeurs éthique de l'entité et les questions d'intégrité et de conflits d'intérêt sont mises en avant dans un document interne ou le personnel est informé par d'autres biais (ex : formation). 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'organisation, 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.*
	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 réglant les éventuels manquements existent, mais la direction n'est pas assurée que le personnel en a connaissance.*	*Des dispositions réglant les éventuels manquements existent et la direction est assurée que l'ensemble du personnel est informé (signature à l'engagement).*	*Des dispositions réglant 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.*

Principes	Critères d'évaluation	*Peu fiable* *N'existe pas ou non appliqué* *1*	*Informel* *Existe mais n'est pas documenté* *2*	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	*Evalué* *Existe de manière développée et documentée* *4*	*Intégré* *Existe de manière optimisée (stratégie et performance)* *5*
A. 5. Attirer, former et fidéliser des personnes compétentes	Il existe une gestion des compétences au sein du service : - formalisation de l'évaluation de la gestion et du développement des compétences nécessaires ; - existence d'une politique de formation et de développement de compétences.	*Les compétences nécessaires sont évaluées au cas par cas, au moment des engagements.*	*La gestion et le développement des compétences nécessaires font l'objet d'une réflexion au sein du service, mais ne sont pas formalisées et sont prises en compte de manière informelle lors d'engagements et de choix de formations.*	*La gestion et le développement des compétences nécessaires sont formalisés et il existe une politique de formation et de développement des compétences.*	*La gestion et le développement des compétences nécessaires sont formalisés et évalués.*	*La gestion et le développement des compétences nécessaires font partie intégrante du processus d'élaboration de la stratégie et évoluent de manière dynamique.*
	Les conditions et principes d'organisation du travail correspondent aux meilleures pratiques et sont en mesure d'attirer et de fidéliser des personnes compétentes.	*Aucune mesure spécifique.*	*Des aménagements du temps de travail, des formations ou d'autres avantages sont octroyés sur demande. La direction est ouverte aux demandes des collaborateurs.*	*Des aménagements du temps de travail, des formations ou d'autres avantages sont octroyés sur la base d'une directive formalisée.*	*Les avantages et l'organisation du travail sont documentés et évalués de manière à correspondre aux besoins des collaborateurs.*	*Les conditions de travail susceptibles d'attirer et de fidéliser les compétences nécessaires font partie intégrante de la stratégie du service, selon une démarche proactive.*
	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.*
	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.*

B. Stratégie et définition des objectifs						
Principes	**Critères d'évaluation**	***Peu fiable*** ***N'existe pas ou non appliqué*** ***1***	***Informel*** ***Existe mais n'est pas documenté*** ***2***	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	***Evalué*** ***Existe de manière développée et documentée*** ***4***	***Intégré*** ***Existe de manière optimisée (stratégie et performance)*** ***5***
B. 6. Analyser le contexte de l'organisation	Une analyse continue et à long terme de la situation et du contexte de l'organisation est effectuée. Les composantes politiques, économiques, sociologiques, technologiques, environnementales et légales sont analysées. Une analyse SWOT (forces, faiblesses, opportunités et menaces) peut par exemple être utilisée.	*Aucune analyse du contexte n'est effectuée.*	*L'analyse du contexte est effectuée de manière informelle et ponctuelle.*	*Il existe une procédure formalisée d'analyse du contexte, mais elle est sommaire.*	*Une analyse détaillée du contexte de l'organisation est réalisée de manière formalisée par la direction et les responsables des différents domaines pour évaluer l'impact potentiel de facteurs internes et externes sur les risques.*	*Un rapport est dressé régulièrement sur les principaux thèmes et tendances qui pourraient influencer et marquer le Canton dans les 10-15 prochaines années. Le recours à des experts issus des milieux scientifique, économique, culturel, politique et administratif permet de déterminer les défis à venir et les perspectives. Le Conseil d'Etat se sert de ce rapport pour définir les priorités politiques (programme de législature).* *De plus, les nouveaux développements, événements et tendances sont analysés et pris en compte dans les objectifs annuels.*
B. 7. Définir l'appétence pour le risque	La direction a conscience de l'importance de prendre des risques appropriés à l'organisation. L'appétence au risque est formalisée.	*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'appétence et de la tolérance au risque de l'organisation et quantification financière du risque résiduel.*
B. 8. Évaluer les stratégies alternatives	L'organisation a établi une stratégie lui permettant d'atteindre ses objectifs, dans le respect de ses missions pérennes et du programme de législature.	*Le service est au clair avec sa mission, mais il n'a pas défini de stratégie. Il adapte la réalisation de ses missions et la mise en œuvre des mesures du programme de législature au fur et à mesure, "au fil de l'eau" .*	*Le service n'a pas formellement défini de stratégie, mais les orientations stratégiques font partie intégrante des séances de direction.*	*Le service établit formellement sa stratégie au moins au début de chaque législature.*	*Le service établit formellement sa stratégie, et vérifie son alignement avec sa vision et ses valeurs.*	*Le service a formalisé un processus stratégique qui intègre la gestion des risques.*
	L'organisation définit des stratégies alternatives pour atteindre les objectifs et évalue leurs impacts potentiels sur le profil de risque.	*Pas de réflexion sur des stratégies alternatives.*	*Des réflexions informelles ont lieu sur des stratégies alternatives visant à atteindre les objectifs.*	*Des réflexions sur les stratégies alternatives qui tiennent compte du profil de risque de l'organisation sont menées et documentées dans les grandes lignes.*	*Une analyse des stratégies alternatives est réalisée et documentée par la direction et les responsables des différents domaines, et l'impact sur les risques est évalué.*	*Le processus stratégique formalisé tient compte des stratégies alternatives et de leur impact sur le profil de risques de l'organisation.*

Principes	Critères d'évaluation	*Peu fiable* *N'existe pas ou non appliqué* *1*	*Informel* *Existe mais n'est pas documenté* *2*	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	*Evalué* *Existe de manière développée et documentée* *4*	*Intégré* *Existe de manière optimisée (stratégie et performance)* *5*
B. 9. Définir les objectifs opérationnels	Les objectifs opérationnels de l'entité sont définis formellement, en ligne avec la stratégie et sont si possible SMART (spécifiques, mesurables, pertinents, réalistes et délimités dans le temps).	*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.*	*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 assurent 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, en lien avec le processus de gestion des risques. Les objectifs sont SMART. Ils tiennent compte de l'appétence et de la tolérance au risque de l'organisation.*
	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 ; ces derniers sont documentés.*	*Les objectifs sont fixés selon un processus clair et développé et réexaminés au moins une fois par législature, en s'assurant de leur cohérence avec la stratégie et l'évolution du contexte.*	*Les objectifs sont fixés selon un processus clair et développé, ils sont revus régulièrement en lien étroit avec le processus de gestion des risques. Ils tiennent compte de l'appétence et de la tolérance au risque de l'organisation.*
	Si des objectifs ont été définis, ils sont déclinés en objectifs d'équipe / individuels et 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 documentés et sont censés être connus de tous, mais la direction ne peut s'en assurer.*	*La communication des objectifs et des résultats fait l'objet d'un processus formalisé.*	*La communication des objectifs et des résultats fait l'objet d'un processus formalisé et intégré dans la gestion de l'organisation, notamment dans sa déclinaison en objectifs d'équipe / individuels.*

C. Performance						
Principes	**Critères d'évaluation**	***Peu fiable*** ***N'existe pas ou non appliqué*** ***1***	***Informel*** ***Existe mais n'est pas documenté*** ***2***	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	***Evalué*** ***Existe de manière développée et documentée*** ***4***	***Intégré*** ***Existe de manière optimisée (stratégie et performance)*** ***5***
C. 10. Identifier les risques	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 est réalisée par la direction uniquement.*	*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.*
	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.*
	Tous les types de facteurs qui influencent les évènements sont considérés : - économiques - environnementaux, - politiques, - sociaux, - technologiques (évènements internes ou externes), - infrastructures, - personnel, - 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.*
	L'inventaire est : - documenté ; - remis à jour régulièrement ; - fait état des interdépendances entre les évènements.	*Il n'existe pas d'inventaire*	*Une réflexion a eu lieu pour lister les risques, mais il n'existe pas d'inventaire documenté*	*L'inventaire est documenté et remis à jour ponctuellement.*	*L'inventaire est documenté et remis à jour régulièrement. 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.*
	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.*

Principes	Critères d'évaluation	*Peu fiable* *N'existe pas ou non appliqué* *1*	*Informel* *Existe mais n'est pas documenté* *2*	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	*Evalué* *Existe de manière développée et documentée* *4*	*Intégré* *Existe de manière optimisée (stratégie et performance)* *5*
C. 11. Évaluer la criticité des risques	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.*
	Une méthode d'estimation du risque a été définie et 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.*
	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 objectifs et la recherche de cohérence sert à maximiser le processus d'évaluation.*
	La fiabilité des données est vérifiée.	*Pas de vérification*	*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.*
	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.*
C. 12. Prioriser les risques	L'organisation a défini des modalités permettant de prioriser les risques.	*Pas de priorisation des risques*	*Les risques sont priorisés sur une base informelle.*	*Les risques sont priorisés selon un processus documenté et la traçabilité de la priorisation est assurée.*	*Le processus de priorisation des risques intègre des critères clairement définis, évalués et revus.*	*Les critères de priorisation des risques sont établis dans le cadre d'un processus intégré de gestion des risques, qui garantit l'alignement entre les risques à considérer et la réalisation de la stratégie.*

Principes	Critères d'évaluation	*Peu fiable* *N'existe pas ou non appliqué* *1*	*Informel* *Existe mais n'est pas documenté* *2*	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	*Evalué* *Existe de manière développée et documentée* *4*	*Intégré* *Existe de manière optimisée (stratégie et performance)* *5*
C. 13. Mettre en œuvre les modalités de traitement des risques	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.*
	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.*
	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.*
	Les réponses aux risques (et opportunités) sont documentées.	*Aucune documentation n'est disponible.*	*Les actions de traitement sont formalisées dans certains documents de manière non coordonnée.*	*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.*
	Les réponses choisies pour adresser les risques sont approuvées par les personnes autorisées et les décisions sont tracées.	*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).*
C. 14. Développer une vision globale du portefeuille de risques	L'organisation dispose d'une vision globale de ses risques et d'une évaluation du portefeuille de ses risques.	*Pas de vision globale des risques.*	*L'organisation dispose d'une vision globale de ses risques sur une base informelle, mais le portefeuille n'est ni documenté, ni réévalué.*	*Le portefeuille des risque est documenté et examiné ponctuellement, lorsque des changements importants sont détectés.*	*Le portefeuille des risque est documenté et examiné régulièrement selon un processus systématique et défini afin de l'adapter aux changements internes et externes.*	*La mise à jour du portefeuille des risques s'inscrit dans un processus global et dynamique, afin de l'adapter au contexte externe et interne de l'organisation et à sa stratégie.*

D. Revue et actualisation						
Principes	**Critères d'évaluation**	***Peu fiable*** ***N'existe pas ou non appliqué*** ***1***	***Informel*** ***Existe mais n'est pas documenté*** ***2***	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	***Evalué*** ***Existe de manière développée et documentée*** ***4***	***Intégré*** ***Existe de manière optimisée (stratégie et performance)*** ***5***
D. 15. Évaluer les changements substantiels *(concentré sur ce qui est nouveau)*	L'organisation identifie et évalue les changements qui pourraient affecter substantiellement la stratégie et les objectifs opérationnels. Pour une détection précoce de risques, les cadres et collaborateurs doivent suivre les changements internes et externes et identifier leurs conséquences possibles en matière de risques. Les risques émergents sont identifiés.	*Pas de processus défini pour l'évaluation des changements et l'identification des risques émergents.*	*Prise en considération au cas par cas des changements substantiels qui surviennent.*	*Les changements substantiels et les risques émergents sont évalués à échéance fixe et documentés.*	*Les changements substantiels et les risques émergents sont identifiés et évalués selon un processus systématique et défini et sont basés sur une analyse ponctuelle et documentée.*	*Veille prospective permettant une identification des changements substantiels et une détection précoce des risques émergents, avec évaluation de l'impact sur la stratégie et les objectifs opérationnels*
D. 16. Réexaminer les risques et la performance *(réexamen de l'actuel, concentré sur le risque résiduel)*	Des évaluations spécifiques ponctuelles de la performance du système de gestion des risques sont effectuées.	*Le système de gestion des risques n'est pas réévalué, il est statique.*	*Le système de gestion des risques est adapté de manière informelle, après des défaillances ou des modifications importantes dans l'organisation*	*Le système de gestion des risques est réévalué selon un processus formalisé et documenté.*	*Le système de gestion des risques est réévalué selon un processus formalisé et documenté, sur la base d'indicateurs de la performance.*	*La réévaluation du système de gestion des risques s'inscrit dans un processus global et dynamique d'évaluation de la stratégie et de la performance.* *(lien avec le SCI et la gestion de la continuité)*
	Le risque résiduel est suivi.	*Pas de suivi du risque résiduel.*	*Le risque résiduel est réévalué après des défaillances ou des sinistres, mais il n'est pas formellement documenté.*	*Le risque résiduel est réestimé de manière ponctuelle et fait l'objet d'une documentation.*	*Le risque résiduel est réévalué selon un processus formalisé et documenté, sur la base d'indicateurs.*	*La réévaluation du risque résiduel s'inscrit dans un processus global et dynamique d'évaluation de la stratégie et de la performance.*
	Un dispositif de pilotage continu est en place afin que la direction soit assurée du bon fonctionnement du système 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 de manière systématique 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.*
D. 17. Poursuivre l'amélioration du management des risques de l'organisation	L'organisation améliore en continu la pertinence, l'adéquation et l'efficacité du cadre organisationnel de management du risque et la façon dont le processus de management du risque est intégré. Lorsque des lacunes ou des opportunités d'amélioration sont identifiées, l'organisme élabore des plans, définit des tâches et les attribue aux responsables de leur mise en œuvre. Une fois mises en œuvre, ces améliorations contribuent au renforcement du management du risque.	*Pas de processus d'amélioration continue du management des risques, le système est statique.*	*Les erreurs ou les inefficiences ne sont pas systématiquement collectées et analysées. Les adaptations se font au cas par cas, de manière individuelle et non partagée. Les propositions d'amélioration proviennent essentiellement de la direction.*	*Les potentiels d'amélioration sont analysés périodiquement ou ponctuellement, sur la base d'un processus documenté. La mise en œuvre d'adaptations ou de nouvelles solutions est effectuée de manière pas toujours coordonnée ou suivie, ponctuellement ou de manière inégale selon les unités. Les propositions d'amélioration continue remontent essentiellement par la voie hiérarchique.*	*Les potentiels d'amélioration sont analysés périodiquement ou ponctuellement, sur la base des outils de reporting à disposition. Les adaptations sont mises en œuvre de manière documentée.*	*L'amélioration continue est un processus organisé, diffusé et intégré par l'ensemble des parties prenantes au sein de l'organisation. Elle est valorisée au sein de l'ensemble des fonctions de l'organisation.* *Lorsque des lacunes ou des opportunités d'amélioration sont identifiées, l'organisme élabore des plans et définit des tâches, et les attribue aux responsables de leur mise en œuvre. Une fois mises en œuvre, ces améliorations contribuent au renforcement du management du risque.*

E. Information, communication et reporting						
Principes	**Critères d'évaluation**	***Peu fiable*** ***N'existe pas ou non appliqué*** ***1***	***Informel*** ***Existe mais n'est pas documenté*** ***2***	***Standard*** ***Existe de manière basique et documentée*** ***3 (norme attendue)***	***Evalué*** ***Existe de manière développée et documentée*** ***4***	***Intégré*** ***Existe de manière optimisée (stratégie et performance)*** ***5***
E. 18. Tirer parti des données et des technologies	Il existe un système d'information fiable, basé sur des technologies performantes, qui assure que les données nécessaires à la réalisation des objectifs soient identifiées, collectées et communiquées.	*Il n'existe pas de système d'information dans l'organisation ou il est inefficace.*	*Système d'information informel (basé sur la tradition orale, au cas par cas), qui exploite peu les nouvelles technologies.*	*Le système d'information est formalisé et repose sur l'utilisation de la technologie, mais pas de manière spécifique pour la gestion des risques.*	*Le système d'information est formalisé et repose sur l'utilisation de la technologie, il est conçu de manière à fournir des informations spécifiques à la gestion des risques.*	*La gestion des risques repose sur un système d'information intégré et interfacé avec les autres systèmes de l'organisation, permettant une gestion performante des données.*
	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 insuffisantes ou de mauvaise qualité (au moins 2 critères non respectés).*	*Les informations sont de manière générale de bonne qualité mais le niveau de qualité n'a pas été défini et la qualité des informations n'est pas formellement vérifiée.*	*Le niveau de qualité des informations a été formellement défini et les informations sont en général conformes aux exigences.*	*Le niveau de qualité des informations a été formellement défini et la qualité des informations est vérifiée au moyen d'indicateurs.*	*La qualité des informations est pilotée et optimisée de manière intégrée et interfacée avec les autres systèmes de l'organisation.*
E. 19. Communiquer les informations relatives aux risques *(à l'interne)*	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 documentée et communiquée aux responsables opérationnels.*	*La stratégie face aux risques et le processus sont communiqués dans toute l'organisation.*	*Communication large dans l'organisation, support du personnel et attitude engagée de la direction (culture d'entreprise).*
	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.*
	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 volonté 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.*
E. 20. Rendre compte des risques, de la culture et de la performance *(à l'externe)*	Une communication adéquate sur la manière de l'organisation de gérer le risque est instaurée à l'externe avec les différentes parties prenantes.	*Pas de communication*	*Réponses sur la manière dont l'entité gère les risques données aux parties prenantes dans le cadre de discussions informelles.*	*Rapport régulier sur la gestion des risques transmis aux parties prenantes.*	*Rapport régulier sur la gestion des risques comprenant des indicateurs transmis aux parties prenantes et prise en compte de leurs réactions pour améliorer le système de gestion des risques.*	*Système de reporting existant prévu dans la politique de gestion des risques.* *Communication externe systématiquement intégrée à la stratégie de communication externe.* *Prise en compte des informations résultant de la consultation des parties prenantes pour améliorer le système de gestion des risques.*

7. La Cour des comptes en bref

La Cour des comptes du canton de Vaud est une autorité indépendante qui a pour mission de contrôler l'utilisation de tout argent public, sous l'angle de la performance en s'assurant principalement du respect des principes d'économie, d'efficacité, d'efficience et de durabilité, et subsidiairement du respect des principes de légalité et de régularité (art. 2 LCComptes).

Ses attributions sont (art. 4 LCComptes) :

- la vérification de la bonne utilisation des fonds des entités soumises à son champ de contrôle ;
- la vérification de l'évaluation de la gestion des risques des entités soumises à son champ de contrôle ;
- le contrôle des subventions accordées par l'Etat ou les communes.

Son champ de contrôle s'étend aux entités suivantes (art. 3 LCComptes) :

- le Grand Conseil et son Secrétariat général ;
- le Conseil d'Etat et son administration ainsi que les entités qui lui sont rattachées ;
- 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 personnes morales de droit public ;
- les personnes physiques et morales auxquelles l'Etat ou une commune délègue l'exécution d'une tâche publique ou accorde, directement ou indirectement, une subvention au sens des articles 7 et 12 de la loi sur les subventions ou une autre contribution au sens de l'article 8, alinéa 1, lettres a,c,d,f,g de la loi sur les subventions.

La Cour des comptes se saisit elle-même des objets qu'elle entend traiter, à l'exception des mandats spéciaux que le Grand Conseil et le Conseil d'Etat peuvent lui attribuer (art. 21 et ss LCComptes).

Elle publie ses rapports pour autant qu'aucun intérêt prépondérant, public ou privé, ne s'y oppose. Ceux-ci consignent ses constatations et recommandations ainsi que les remarques de l'entité auditée. Ils sont consultables sur le site Internet de la Cour : www.vd.ch/cdc.

Dans son rapport annuel, la Cour des comptes doit mentionner ses recommandations ainsi que les suites qui leur ont été données. Les entités auxquelles des recommandations ont été adressées doivent prendre position par écrit.

Toute personne peut communiquer à la Cour des signalements en rapport avec des faits entrant dans ses attributions. La Cour des comptes est libre d'y donner suite ou non.

Vous pouvez apporter votre contribution au bon usage de l'argent public en contactant la Cour des comptes :

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