



# **MANUEL DE VERIFICATION DE L'EVALUATION DE LA GESTION DES RISQUES**

**Méthodologie d'audit  
de la Cour des comptes du Canton de Vaud**

**Volume 3**

**septembre 2009**

Cour des comptes du canton de Vaud  
Rue de Langallerie 11 – 1014 Lausanne  
Téléphone : 021 316 58 00 – fax : 021 316 58 01  
Courriel : [info.cour-des-comptes@vd.ch](mailto:info.cour-des-comptes@vd.ch)  
[www.vd.ch/cdc](http://www.vd.ch/cdc)



## TABLE DES MATIERES

<b>Introduction</b>	<b>5</b>
<b>Chapitre 1</b>	
<b>Cadre général des activités de la Cour des comptes</b>	<b>7</b>
1.1. Aspects légaux	7
1.2. Champ d'intervention	8
1.2.1. Champ de contrôle	9
1.2.2. Objectifs de contrôle et types d'audit	9
1.2.3. Types de missions	12
1.2.4. Synthèse des missions et objectifs de contrôle	14
<b>Chapitre 2</b>	
<b>La gestion des risques</b>	<b>16</b>
2.1. Contexte général	16
2.1.1. Les récents développements légaux	17
2.1.2. La mission de vérification de l'évaluation de la gestion des risques de la Cour des comptes	18
2.2. Définition générale de la gestion des risques	20
2.2.1. La définition proposée par le COSO	20
2.2.2. L'application au secteur public	20
2.3. Le modèle de gestion des risques de référence pour la Cour des comptes	22
2.3.1. Les objectifs	23
2.3.2. Le champ de contrôle	23
2.3.3. Les composantes de la gestion des risques	24

<b>Chapitre 3</b>	
<b>La méthodologie des missions de vérification de l'évaluation de la gestion des risques</b>	<b>31</b>
3.1. Aperçu de la méthodologie	32
3.2. La phase de proposition du thème de l'audit	34
3.3. La phase de planification de l'audit	37
3.3.1. L'étude préliminaire	39
3.3.2. Le plan d'audit	40
3.3.3. Le rapport d'étude préliminaire	42
3.4. La phase d'exécution de l'audit	44
3.4.1. L'annonce de l'audit	46
3.4.2. La séance d'ouverture de l'audit	46
3.4.3. L'exécution des procédures d'audit	46
3.4.4. La rédaction des constatations et la formulation des recommandations	47
3.4.5. Le projet de rapport	49
3.5. La phase de publication du rapport final	54
3.6. Le suivi du rapport	56
<b>Annexes</b>	<b>57</b>

## Introduction

En s'acquittant de ses missions, la Cour des comptes du Canton de Vaud (ci-après « la Cour des comptes ») peut être confrontée à des situations comportant une grande diversité et une importante complexité, de par la nature même des types d'audits effectués, de par la diversité de son champ de contrôle et de par la latitude laissée à l'auditeur dans ses appréciations et ses interprétations.

La mise en place d'une méthodologie est dès lors indispensable afin de pouvoir adopter une approche structurée, avec pour objectifs :

- la réalisation de contrôles objectifs et fiables ;
- le maintien et le développement d'un haut niveau de compétence ;
- la mise à disposition d'un outil propre à mesurer l'efficacité, l'économie et l'efficience des contrôles ;
- la possibilité pour les tiers d'avoir une meilleure vision des méthodes et du professionnalisme de la Cour des comptes, renforçant ainsi sa crédibilité, ainsi que la bonne compréhension de ses activités.

La méthodologie d'audit de la Cour des comptes se fonde sur les normes de contrôle et lignes directrices établies par l'Organisation internationale des Institutions supérieures de contrôle des finances publiques (INTOSAI<sup>1</sup>), sur les bonnes pratiques actuelles dans le domaine de l'audit et de l'évaluation des institutions publiques (dont la Cour des comptes européenne, le Bureau du vérificateur général du Canada et le Contrôle fédéral des finances<sup>2</sup>) et enfin sur le *Code de déontologie et Directives relatives à la qualité des audits* édicté par la Cour des comptes elle-même.

La méthodologie de la Cour des comptes est exposée de manière détaillée dans le *Manuel de méthodologie générale de la Cour des comptes du Canton de Vaud*. Le présent document a pour objectif de présenter de manière plus spécifique la méthodologie adaptée aux missions de vérification de l'évaluation de la gestion des risques, l'une des trois attributions générales conférées par la loi à la Cour des comptes.

Ce document a été rédigé de manière à ce que les lecteurs soient en mesure de comprendre l'essentiel de la méthodologie sans avoir lu préalablement la totalité du manuel ci-dessus. Les fondamentaux de la méthodologie générale sont résumés au chapitre 3.

Le présent manuel se structure en trois chapitres :

Présentation du cadre général des activités de la Cour des comptes du Canton de Vaud.

Exposé des bases théoriques générales relatives à la gestion des risques et du modèle adopté par la Cour des comptes pour ses audits.

- 
1. Pour plus d'informations : <http://www.intosai.org>
  2. Pour plus d'informations :
    - Cour des comptes européenne : <http://eca.europa.eu>
    - Bureau du vérificateur général du Canada : <http://www.oag-bvg.gc.ca>
    - Contrôle fédéral des finances : <http://www.efk.admin.ch>

Présentation résumée de la méthodologie de la Cour des comptes et exposé des travaux de contrôle spécifiques à ses missions de vérification de l'évaluation de la gestion des risques.

Le présent document a été approuvé par la Cour en séance plénière le 24.09.2009.

Le Président :  
Jean-Claude Rochat

La Vice-présidente :  
Anne Weill-Lévy

# CHAPITRE 1

## CADRE GENERAL DES ACTIVITES DE LA COUR DES COMPTES

Le présent chapitre a pour objectif de présenter d'une part le cadre général dans lequel évolue la Cour des comptes du canton de Vaud (paragraphe 1.1) et d'autre part son champ d'intervention (paragraphe 1.2). La dernière partie de ce chapitre (paragraphe 1.3) expose également le lien entre ces éléments et le plan stratégique établi par la Cour sur une base triennale.

### 1.1 Aspects légaux

L'existence, la mission et l'indépendance de la Cour des comptes du Canton de Vaud trouvent leurs fondements dans la loi.

#### 1) Constitution Vaudoise

« *La Cour des comptes assure en toute indépendance le contrôle de la gestion des finances des institutions publiques désignées par la loi ainsi que de l'utilisation de tout argent public, sous l'angle de la légalité, de la régularité comptable et de l'efficacité* » (art. 166. al. 2).

#### 2) Loi sur la Cour des comptes du 21 novembre 2006 (LCCComptes)

« *La Cour des comptes assure en toute indépendance le contrôle de la gestion des finances des institutions publiques désignées par la présente loi ainsi que de l'utilisation de tout argent public, sous l'angle de la légalité, de la régularité comptable et de l'efficacité* » (art. 2).

L'exposé des motifs de juin 2006 sur la Cour des comptes précise que « *c'est ce dernier critère, soit celui de l'efficacité, qui sera prépondérant dans le cadre de l'accomplissement des contrôles de la Cour des comptes* ». Le contrôle des institutions publiques sous l'angle de l'**efficacité** consiste en :

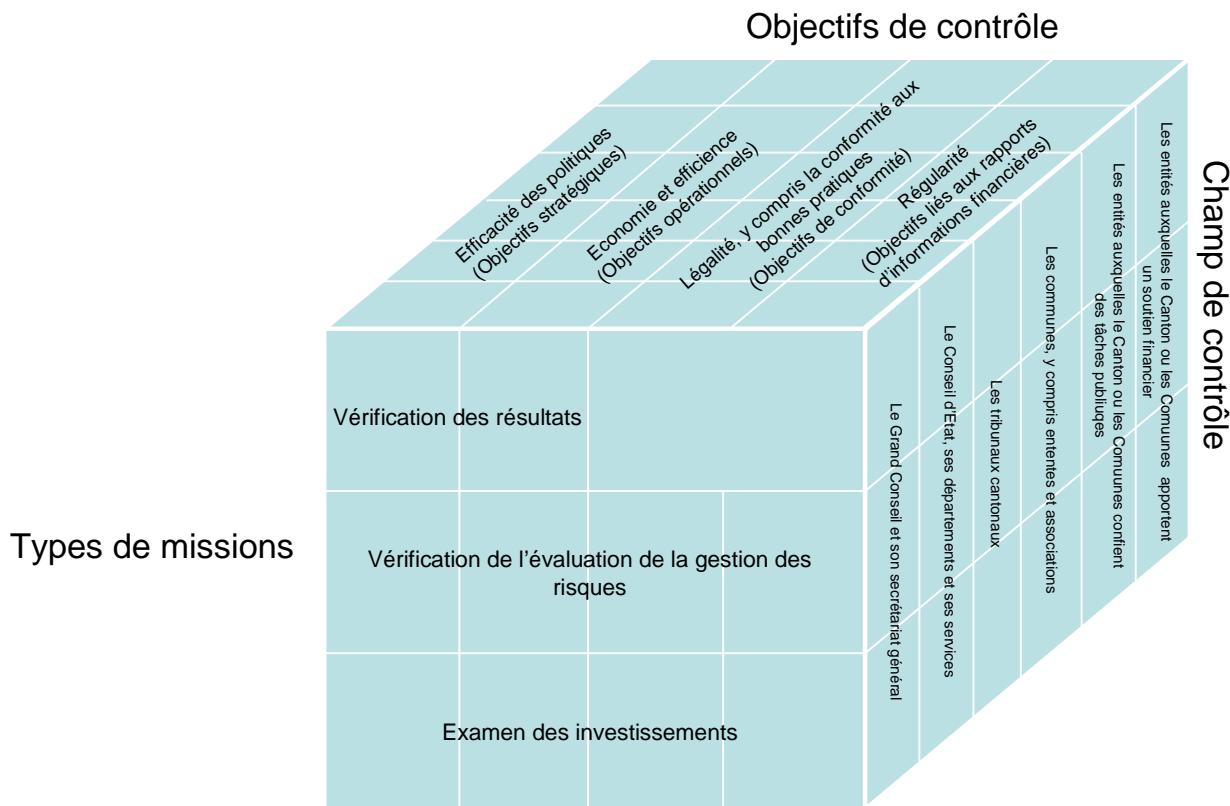
- la vérification par la Cour des comptes du respect des principes d'**économie** et d'**efficience** lors de l'acquisition, de la gestion et de la production des biens et services publics ;
- la mesure de l'**efficacité** des politiques publiques.

Les attributions générales de la Cour des comptes sont définies à l'art. 24 : « *La Cour des comptes procède*

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

Conformément à ce qui est mentionné dans l'exposé des motifs, la Cour des comptes ne procède pas à des appréciations sur l'opportunité politique d'une mesure, ni sur la légitimité d'une dépense<sup>3</sup>.

## 1.2. Champ d'intervention



3. *Exposé des motifs et projet de loi sur la Cour des comptes* (juin 2006), pages 5, 28 et 42

Le champ d'intervention de la Cour des comptes du Canton de Vaud peut être modélisé par le cube ci-dessus, dont les axes sont les suivants :

- l'ordonnée reflète les entités soumises au champ de contrôle de la Cour des comptes ;
- l'abscisse représente les principes de base qui sous-tendent tout contrôle de la Cour, regroupés en fonction des objectifs COSO (voir point 2.2) ;
- l'axe vertical représente les trois types de missions de la Cour.

Chacun de ces axes est explicité dans les sous-chapitres suivants.

### **1.2.1. Champ de contrôle**

Le champ de contrôle de la Cour des comptes<sup>4</sup> s'étend aux entités suivantes :

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

### **1.2.2. Objectifs de contrôle et types d'audit**

Les contrôles de la Cour des comptes sont effectués sous l'angle des principes de légalité, de régularité, d'économie, d'efficience et d'efficacité<sup>5</sup>. Ces principes peuvent être définis de la manière suivante :

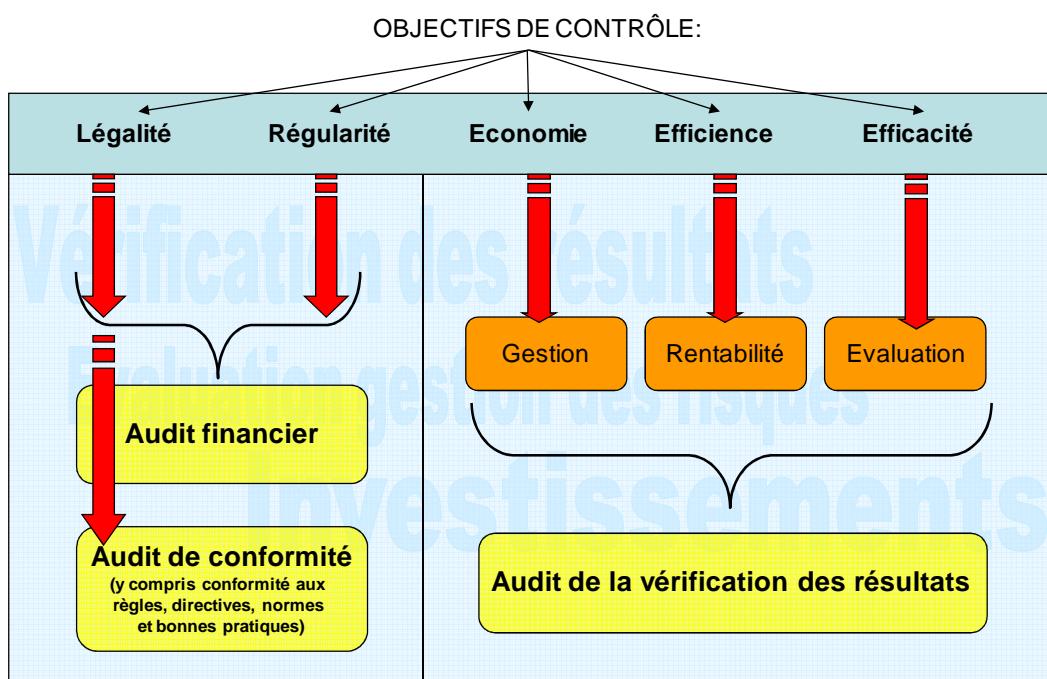
---

4. Art. 28 de la LCComptes

5. Conformément à l'art. 2 LCComptes (mission) et à l'art. 3 Loi sur les finances (LFin) (principes généraux)

- 1) Principe de légalité : toute dépense et toute recette doit être fondée sur une base légale<sup>6</sup>.
- 2) Principe de régularité : la comptabilité doit être à jour, organisée systématiquement et de manière rationnelle.
- 3) Principe d'économie : les ressources engagées doivent être utilisées de manière économe.
- 4) Principe d'efficience : la relation entre les ressources engagées et les résultats obtenus est avantageuse.
- 5) Principe d'efficacité : les résultats obtenus ont l'effet escompté.
- } Principe des « 3 E »

Dans le cadre de chacune de ses missions, la Cour des comptes doit détecter les risques potentiels pour la légalité, la régularité, l'économie, l'efficience et l'efficacité et choisir le type d'audit le plus approprié pour y parvenir. Ainsi, la Cour des comptes peut mener les audits<sup>7</sup> suivants, catégorisés selon leur(s) objectif(s) de contrôle :



6. *Exposé des motifs et projet de loi sur la Cour des comptes*, p. 41

7. Le terme « audit » est utilisé indistinctement pour désigner les différentes missions de contrôle de la Cour.

## 1) Audit financier

Vérification des états financiers d'une entité publique comprise dans le champ de contrôle de la Cour des comptes, ainsi que de la légalité et de la régularité des opérations sous-jacentes.

## 2) Audit de conformité

Vérification de la conformité des opérations ou des systèmes aux lois et règlements, aux directives, aux normes et aux bonnes pratiques en vigueur.

L'audit de conformité peut être un élément-clé de l'audit financier, mais il peut également s'étendre à la conformité des opérations ou des systèmes au-delà du cadre purement financier.

## 3) Audit de la vérification des résultats

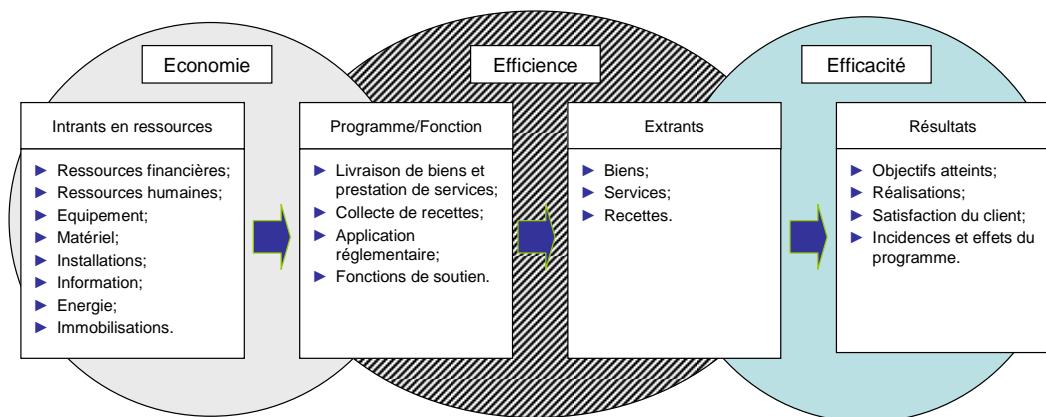
La nature de l'audit de la vérification des résultats (appelé également audit de la performance) est définie par rapport au principe des « 3 E » (Économie, Efficience et Efficacité). Le chapitre 1.2.3. ci-après décrit plus spécifiquement ce type d'audit.

### 1.2.3. Types de missions

Selon les attributions qui lui ont été conférées par la loi<sup>8</sup>, les missions spécifiques de la Cour des comptes du Canton de Vaud comportent trois domaines essentiels :

#### 1) La vérification des résultats

La vérification de résultats (appelée également « audit de la performance ») est l'examen indépendant de l'application des principes d'économie, d'efficience et d'efficacité (principe des « 3 E » des programmes, organisations et entreprises du secteur public dans la perspective de réaliser des améliorations).



Les *intrants* sont les ressources engagées alors que les *extrants* sont les prestations fournies par l'entité.

La vérification des résultats consiste en une combinaison de deux au moins des types d'audit suivants :

Audit de gestion :

examen des **économies** réalisées (intrants) dans la gestion des entités contrôlées, conformément à des pratiques et des principes opérationnels sains et une bonne politique de gestion.

Audit de rentabilité :

contrôle de l'**efficience** des processus mis en œuvre dans les entités contrôlées, c'est-à-dire l'analyse de la rentabilité de l'utilisation des ressources humaines, financières (intrants) ou autres par rapport au produit ou à la prestation fournis par l'entité contrôlée (extrants). C'est en d'autres termes l'examen du rapport entre les intrants et les extrants.

8. Art. 24 LCCComptes

**Audit d'évaluation :**

appréciation de l'**efficacité** d'une politique publique, d'un programme ou d'un projet, en se concentrant sur les liens de causalité entre d'une part les objectifs et d'autre part la réalisation et les effets de la politique, du programme ou du projet examinés (extrants). C'est en d'autres termes l'examen du rapport entre les extrants et les objectifs fixés.

La Cour des comptes choisit d'utiliser l'approche ou la combinaison d'approche d'audits qui produit les résultats les plus utiles en regard des ressources à mettre en œuvre.

Ce type de mission est décrit dans le *Manuel de la vérification des résultats*.

## **2) La vérification de l'évaluation de la gestion des risques**

La Cour des comptes a pour mission de vérifier l'évaluation de la gestion des risques effectuée dans les entités soumises à son champ de contrôle.

Cette vérification consiste à analyser si un processus de gestion des risques est élaboré et mis en œuvre conformément aux normes et aux bonnes pratiques en vigueur. Elle est pour une part un audit de conformité, mais également un audit de vérification des résultats puisqu'elle porte aussi sur l'efficacité, l'économie et l'efficience du processus de la gestion des risques.

Le présent manuel expose en quoi consiste ce type d'audits et quelle est la méthodologie suivie par la Cour pour leur exécution.

## **3) L'examen des investissements**

L'examen des investissements qui bénéficient de subventions, de prêts ou de garanties publiques (y. c. les investissements propres de l'État et des communes) consiste à examiner dans quelle mesure l'argent public y est investi conformément aux principes de légalité, de régularité, d'économie, d'efficience et d'efficacité.

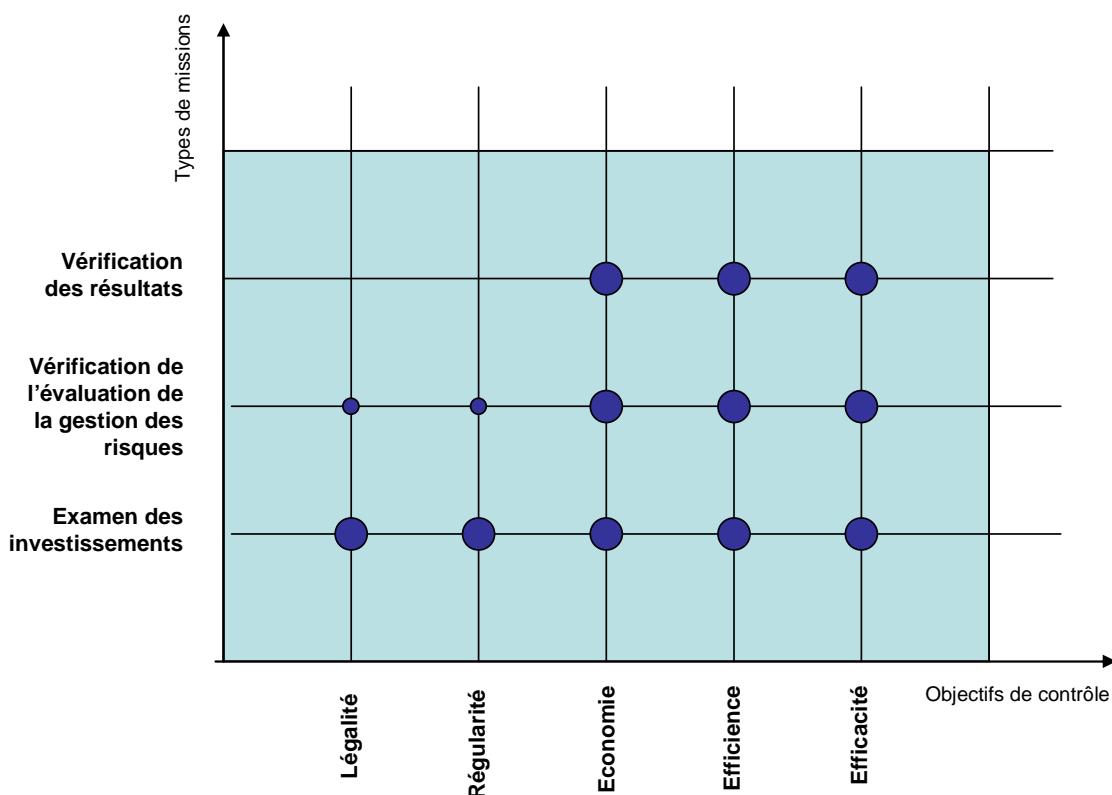
La méthodologie relative à ce type de mission est exposée dans le *Manuel de l'examen des investissements*.

## 1.2.4. Synthèse des missions et objectifs de contrôle

Il découle des objectifs de contrôle (cf. 1.2.2) et des trois attributions de la Cour (cf. 1.2.3) présentés ci-dessus les types d'audit suivants :

- audit financier ;
- audit de conformité (ou de *compliance*) ;
- audit de vérification des résultats (ou de performance) ;
- audit de gestion ;
- audit de rentabilité ;
- audit d'évaluation ;
- audit de vérification de l'évaluation de la gestion des risques ;
- audit de l'examen des investissements.

Ces possibilités sont schématisées dans le diagramme ci-dessous par les points bleus. Pour chaque type de mission, les objectifs prioritaires sont marqués d'un point bleu plus important.



Lorsque plusieurs types d'audit apparaissent dans un contrôle, ce dernier est placé dans la catégorie dominante.

Quel que soit le type d'audit réalisé, les contrôles de la Cour des comptes ne portent en tout cas pas sur l'opportunité politique d'une mesure. Les contrôles de la Cour des comptes interviennent en principe *a posteriori* et ne portent en aucun cas sur la légitimité de la dépense.

## CHAPITRE 2

# LA GESTION DES RISQUES

Le présent chapitre a pour objectif de situer la gestion des risques dans le contexte actuel (paragraphe 2.1.), puis de définir d'une part en quoi consiste la gestion des risques de manière générale (paragraphe 2.2.) et, d'autre, part le modèle de référence de gestion des risques de la Cour des comptes (paragraphe 2.3.).

### 2.1. Contexte général

Le secteur public doit faire face à un environnement toujours plus complexe et à des attentes toujours plus significatives de la part des citoyens et des divers partenaires. Il se trouve confronté à des défis tels que la demande croissante de services publics de qualité, l'efficacité accrue en matière de fourniture des prestations, une gestion administrative responsable et la diversité du catalogue des tâches dans un environnement fait de restrictions budgétaires, de nombreuses normes et de recherche de performance.

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

La gestion des risques vise non seulement à apporter une réponse efficace aux risques et aux opportunités associés aux incertitudes, renforçant ainsi la capacité de l'organisation de réaliser sa mission et ses objectifs, mais aussi à lui permettre de fournir des services plus efficaces, de manière plus efficiente et économique, tout en tenant compte de valeurs telles que l'équité et la justice.

La maîtrise des risques est ainsi à considérer aujourd'hui comme un élément-clé dans la conduite des missions du secteur public. Les développements survenus dans le secteur privé en matière de politique de gestion des risques sont désormais suivis également par le secteur public.

## 2.1.1. Les récents développements légaux

L'importance croissante des questions relatives à la gestion des risques se retrouve dans les différents développements légaux intervenus récemment dans le secteur public, sous l'impulsion des évolutions touchant le secteur privé.

### Dans le secteur privé

L'**art. 663b ch. 12 du Code des obligations**, entré en vigueur au 1<sup>er</sup> janvier 2008, stipule que l'annexe aux comptes annuels doit contenir « *des indications sur la réalisation d'une évaluation du risque* ». L'objectif de cette disposition est d'introduire une surveillance préventive consistant à évaluer la tendance de l'évolution des affaires et la nécessité d'intervenir pour changer de cap ainsi qu'à identifier et à estimer les principaux risques auxquels la société est exposée et qui pourraient menacer dans un avenir prévisible ses résultats.<sup>9</sup> Diverses entités du champ de contrôle de la Cour des comptes sont désormais soumises à cet article.

### Dans le secteur public

#### a) Sur le plan fédéral

Directement inspiré des nouvelles dispositions du Code des obligations, l'**article 3 de l'Ordonnance du 5 avril 2006 sur les finances de la Confédération (OFC)** prévoit (en application de l'art. 10 d) de la Loi sur les finances de la Confédération (LFC), que l'annexe des comptes annuels doit contenir « *des données complémentaires sur les risques et la gestion des risques* ».

L'art. 50 (en application de l'art. 39 LFC) stipule quant à lui que :

- « 1 Les départements et la Chancellerie fédérale gèrent les risques dans leur domaine de compétence selon les directives du Conseil fédéral.
- 2 En principe, la Confédération assume le risque pour les dommages causés à son patrimoine et supporte les conséquences de son activité.
- 3 L'Administration des finances édicte des directives sur :
  - a. la conclusion de contrats d'assurance dans des cas particuliers ;
  - b. la prise en charge contractuelle de la responsabilité civile pour les dommages à des tiers ;
  - c. l'indemnisation volontaire pour des dommages matériels que des agents fédéraux subissent dans le cadre de l'exercice de leurs fonctions ;
  - d. le règlement financier de dommages matériels et pécuniaires.

---

9. Article « Évaluation des risques et systèmes de contrôle interne » par B. Chapuis et B. Perrin, *L'expert comptable suisse*, numéro 9/2008

4 Elle coordonne l'établissement des rapports destinés au Conseil fédéral. »

*b) Sur le plan du Canton de Vaud*

Le seul article de loi faisant référence à l'évaluation des risques est l'art. 15 al. 2 i) de la Loi sur les finances (LFin) qui stipule que le Département des finances a la compétence d'évaluer les risques financiers. Cependant, **aucun article de loi** n'impose actuellement aux départements de l'État de mener et de fournir des informations relatives à leur gestion des risques. Au contraire du *Code des obligations* et de l'*Ordonnance sur les Finances de la Confédération*, l'art. 49 relatif à l'annexe aux comptes ne requiert pas à ce jour d'informations relatives à l'évaluation des risques.

*c) Sur le plan des communes vaudoises*

Aucune exigence en matière d'évaluation des risques ne figure dans les lois et règlements en vigueur.

Malgré l'absence d'exigence légale et compte tenu du fait que la vérification de l'évaluation de la gestion des risques constitue l'une des attributions de la Cour des comptes, on peut en déduire qu'il est attendu des entités publiques qu'elles procèdent à une gestion de leurs risques. La maîtrise de ceux-ci leur permet en effet de gérer avec plus d'efficience et d'efficacité les deniers publics.

## **2.1.2. La mission de vérification de l'évaluation de la gestion des risques de la Cour des comptes**

La vérification de l'évaluation de la gestion des risques est l'une des trois attributions générales de la Cour des comptes (voir paragraphe 1.2.3.). La Cour des comptes entend, à travers cette mission, encourager et soutenir les entités publiques dans la gestion et la maîtrise de leurs risques.

Comme indiqué dans *l'Exposé des motifs du projet de loi sur la Cour des comptes*, la Cour des comptes n'a pas, dans le cadre de ce type de mission, à procéder elle-même à cette évaluation, mais doit « vérifier si l'évaluation menée par l'audité répond aux critères de légalité, de régularité comptable et d'efficacité »<sup>10</sup>. Ses travaux sont ainsi destinés à valider l'existence et à évaluer la pertinence du **processus de gestion des risques** de l'entité pour les risques de ses activités.

Conformément aux objectifs de contrôle de la Cour (paragraphe 1.2), la vérification de l'évaluation de la gestion des risques doit s'orienter autour des quatre catégories possibles de **risques majeurs** selon le modèle COSO<sup>11</sup> :

- **Les risques relatifs aux objectifs stratégiques** (efficacité des politiques) : ils sont caractérisés par le fait que, s'ils se réalisent, la stratégie de l'entité pourrait ne pas être conduite avec efficacité. Les objectifs stratégiques sont des objectifs de niveau élevé, en ligne avec la mission de l'entité. La mission du secteur public est de fournir des prestations destinées à servir l'intérêt général.

10. *Exposé des motifs et projet de loi sur la Cour des comptes*, p.42

11. Committee of Sponsoring Organizations of the Treadway Commission

- **Les risques relatifs aux objectifs opérationnels** (économie et efficience) : ceux-ci concernent la structure, l'organisation et le fonctionnement de l'entité. S'ils se réalisent, ils peuvent avoir une incidence directe sur la qualité et la quantité des prestations fournies, sur l'activité courante, voire sur la poursuite de l'activité.
- **Les risques relatifs aux objectifs de conformité** (légalité, y compris la conformité aux bonnes pratiques) : ils sont liés au respect ou non des dispositifs légaux et réglementaires, voire de l'application de règles de gouvernance et de bonnes pratiques. Ils sont également de nature à engager la responsabilité civile et/ou pénale de l'entité concernée.
- **Les risques relatifs aux objectifs liés aux rapports d'informations financières** (régularité) : ces risques peuvent affecter la maîtrise des flux financiers de l'entité. Les conséquences se font directement sentir sur les comptes, la qualité des informations financières, la capacité à maintenir et développer le patrimoine, la fiabilité des recettes, la maîtrise des investissements et la gestion de la trésorerie.

À l'intérieur de ces risques majeurs existent en particulier trois autres **risques spécifiques** qui sont :

- **Le risque de contrôle** : il est lié à l'inadéquation des procédures de contrôle, à leur inexistence ou à leur non-application ;
- **Le risque d'irrégularités, de fraude et de corruption** : il caractérise des situations en général à caractère pénal qui peuvent affecter gravement l'ensemble de l'activité de l'entité ;
- **Le risque d'image** : ce risque est lié à la crédibilité de l'entité et à la façon dont elle est perçue par son environnement interne et externe. Il est de nature à affecter notamment le degré d'acceptation nécessaire à la mobilisation des ressources humaines et financières.

La méthodologie présentée ci-après a été développée spécifiquement dans le but de la vérification de l'évaluation de la gestion des risques stratégiques, opérationnels et de conformité. La Norme d'audit suisse 890 (NAS 890) règle quant à elle spécifiquement la vérification de l'existence du système de contrôle interne relatif à l'établissement des comptes annuels (et par conséquent la gestion des risques relatifs à ce processus).

Précisons à ce sujet que l'article 59 lit. f de la LFin prévoit que le Contrôle cantonal des finances est compétent pour la « *certification du système de contrôle interne de l'État* » (relatif à l'établissement des comptes annuels). Dès lors, la Cour des comptes ne se penche en principe pas sur les risques relatifs au processus d'établissement des comptes annuels pour les entités de son champ de contrôle qui sont déjà soumises au champ de contrôle du Contrôle cantonal des finances (le Grand Conseil et son Secrétariat général ; le Conseil d'État, ses départements et ses services ; le Tribunal cantonal ainsi que les tribunaux et autres offices qui lui sont rattachés). Concernant les autres entités soumises à son champ de contrôle, qui ne font pas l'objet d'une vérification de l'existence du

système de contrôle interne relatif aux comptes annuels<sup>12</sup>, la Cour des comptes peut décider de mener un audit spécifique sur ce sujet, sur la base d'une approche d'audit adaptée, non développée dans le présent manuel.

## 2.2. Définition générale de la gestion des risques

### 2.2.1. La définition proposée par le COSO

Parmi les différents modèles de gestion des risques<sup>13</sup>, la Cour a choisi comme référence le modèle COSO, celui-ci étant la référence reconnue par INTOSAI et par la Confédération. La définition de la gestion des risques qu'il propose est délibérément large, afin de couvrir autant de secteurs et de types d'organisation que possible.

*« La gestion des risques des entités est un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation »<sup>14</sup>.*

### 2.2.2. L'application au secteur public

Comme le relève la Confédération dans sa politique de gestion des risques, toute entité publique devrait disposer d'une politique de gestion des risques qui :

- permette de déterminer une approche homogène et systématique des divers risques encourus,
- fasse partie intégrante des obligations de diligence que les départements et les unités administratives doivent remplir dans le cadre de leurs activités,
- soutienne les départements et les unités administratives dans l'exercice efficace de leurs tâches, et
- fournisse des instruments et des mesures pour identifier, évaluer, maîtriser et surveiller les risques potentiels avec cohérence et efficacité.

---

12. Soit les communes, ainsi que les ententes, associations, fédérations et agglomérations de communes; les corporations, établissements, associations, fondations, sociétés et autres entités auxquels le canton ou une commune confie des tâches publiques ou apporte un soutien financier, que ce soit par des subventions, des aides financières ou des indemnités ou pour lesquels il constitue des cautionnements ou des garanties.

13. Citons à titre d'exemples la norme ISO 31000, publiée en 2009 par l'Organisation Internationale de Normalisation, qui fournit des principes et des lignes directrices générales sur le management du risque, ou encore le Cadre de référence de la gestion des risques, proposé par la Federation of European Risk Management Associations (FERMA).

14. COSO — Modèle ERM 2004 — *Modèle global de gestion des risques des entités*

Il ressort de la définition figurant sous le paragraphe 2.2.1. que la gestion des risques dans le secteur public est<sup>15</sup> :

- un **processus**, c'est-à-dire un enchaînement itératif et continu d'actions intégrées et non un dispositif statique représentant un effort de management additionnel ;
- déployée par **l'ensemble des collaborateurs**, puisqu'elle est mise en œuvre par la direction et les collaborateurs sous la supervision de la haute direction et influence les actes de chacun ;
- prise en compte dans l'élaboration de la **stratégie** puisque la haute direction examine une stratégie et ses alternatives en fonction des risques associés ;
- appliquée dans **toute l'organisation**, puisque tous les niveaux, de la planification stratégique aux opérations des divers processus, sont examinés ;
- adaptée à **l'appétence pour le risque**, soit le niveau de risque global auquel la direction de l'entité accepte de faire face dans la réalisation de sa mission et de ses objectifs ;
- un dispositif donnant les moyens à la haute direction d'obtenir une **assurance raisonnable**, et non totale, puisque l'avenir ne peut être prédit avec précision ;
- un moyen d'atteindre des **objectifs** et non une fin en soi.

Les objectifs de la gestion des risques peuvent être définis comme suit<sup>16</sup> :

- soutenir les instances dirigeantes au moyen d'informations sur les risques complètes, transparentes et actualisées (aide à la décision) ;
- avoir une vue d'ensemble de la situation en matière de risques et une conscience élevée des risques à tous les niveaux de l'entité (outil de communication) ;
- contrôler et réduire au minimum les coûts des risques ;
- garantir un niveau élevé de sécurité physique pour les personnes et valeurs patrimoniales ;
- exécuter des tâches axées sur les résultats, la rentabilité et l'anticipation ;
- maintenir le bon fonctionnement de l'entité en tout temps ;
- préserver la bonne réputation de l'entité en son propre sein, dans le public et vis-à-vis de ses autres interlocuteurs.

---

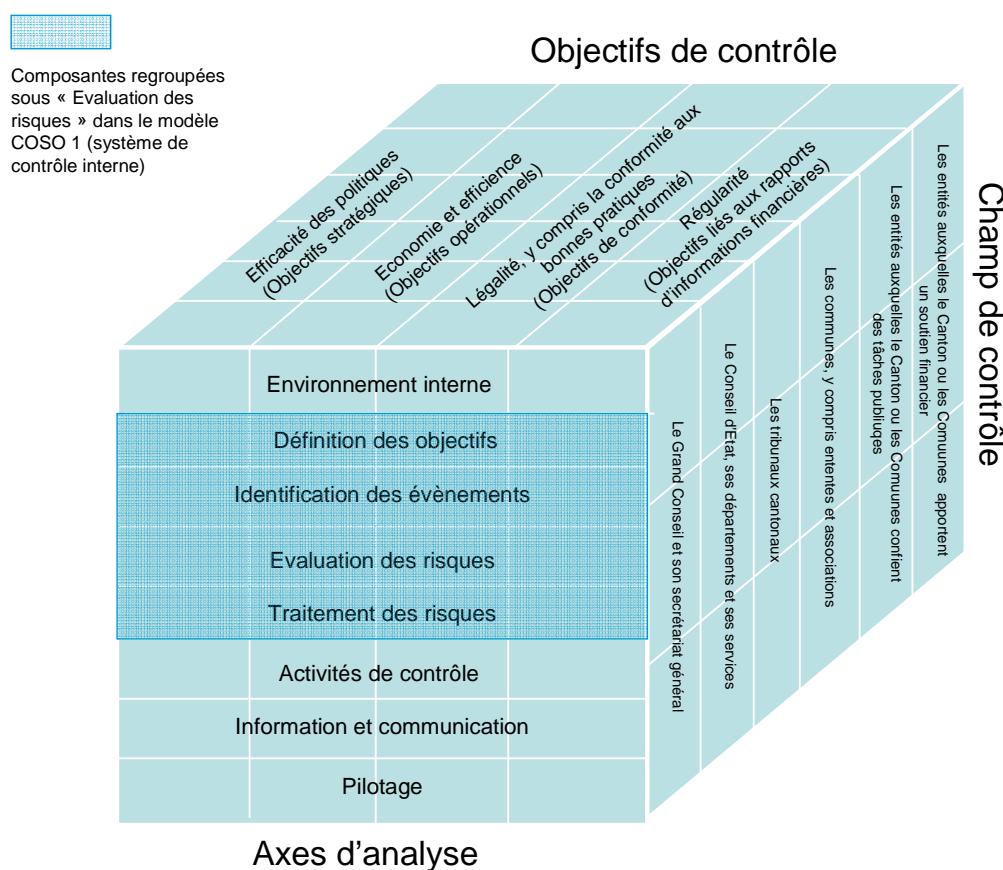
15. COSO II Report — *Le management des risques de l'entreprise*

16. « Politique de gestion des risques » de la Confédération

## 2.3. Le modèle de gestion des risques de référence pour la Cour des comptes

La gestion des risques des entités repose sur la mission et la vision définie par l'organisation. Dans le cadre de cette mission, la direction devrait déterminer les objectifs stratégiques, concevoir les processus pour atteindre ces objectifs et décliner les objectifs secondaires qui en découlent à tous les niveaux de l'organisation.

En transposant le modèle COSO II (relatif à la gestion des risques), adapté au secteur public, dans ses lignes directrices, la Cour des comptes du Canton de Vaud a défini les éléments d'un processus « modèle » de gestion des risques. Ce cadre lui sert de référence pour évaluer l'efficacité du dispositif de gestion des risques des entités entrant dans son champ de contrôle.



La face supérieure du cube représente les catégories d'objectifs de la vérification de l'évaluation de la gestion des risques. La face frontale du cube représente les axes d'analyse du processus de gestion des risques. La face latérale du cube reflète quant à elle les entités soumises au champ de contrôle de la Cour des comptes. Ces différents éléments sont expliqués plus en détail ci-après.

## Lien entre le contrôle interne et la gestion des risques des entités

À bien des égards, la gestion des risques des entités peut être considérée comme une évolution naturelle du modèle de contrôle interne. La plupart des organisations tendront à appliquer entièrement le modèle de contrôle interne (COSO I) avant de mettre en œuvre les concepts inhérents à la gestion des risques des entités, dont le contrôle interne fait intégralement partie.

Le modèle de gestion des risques des entités comprend ainsi le contrôle interne, mais représente en outre une conceptualisation plus approfondie de la manière dont les décisions de gestion prises par une organisation devraient dériver ; de plus, il représente un outil susceptible d'aider la direction de l'entité à déterminer la réponse correcte face à un événement particulier.

### 2.3.1. Les objectifs

Selon les *Lignes directrices de l'INTOSAI sur les normes de contrôle interne à promouvoir dans le secteur public*, on peut classer les objectifs dans les quatre catégories suivantes :

- a) *les objectifs stratégiques* :  
ces objectifs servent la mission de l'organisation et se reflètent dans les objectifs des politiques publiques ;
- b) *les objectifs opérationnels* :  
ces objectifs visent l'exécution d'opérations ordonnées, éthiques, économiques, efficientes et efficaces et la protection des ressources contre le risque d'image, les pertes, les mauvais usages, les dommages et la fraude ; ils ont trait au fonctionnement de l'entité, à ses processus internes ;
- c) *les objectifs relatifs aux rapports d'informations financières* :  
ces objectifs sont liés à la fiabilité des informations rapportées et au respect des obligations de rendre compte ;
- d) *les objectifs de conformité* :  
il s'agit d'objectifs visant la conformité aux lois et réglementations en vigueur et de capacité d'action conforme à la politique gouvernementale ; il ne s'agit pas de préciser des objectifs de conformité à chaque loi, règlement et directive en vigueur, mais de se situer à un niveau qui concerne les lois et règlements principaux en lien avec la mission de l'entité (par exemple la Loi sur les marchés publics).

### 2.3.2. Le champ de contrôle

Pour chacune des entités faisant partie du champ de contrôle de la Cour des comptes, il est possible de subdiviser encore cette dimension en fonction de son organisation, par exemple en « services » pour un département de l'État.

### **2.3.3. Les composantes de la gestion des risques**

Le processus de gestion des risques comprend huit éléments interdépendants définis ci-après :

- l'environnement interne (2.3.3.1) ;
- la définition des objectifs (2.3.3.2) ;
- l'identification des événements (2.3.3.3) ;
- l'évaluation des risques (2.3.3.4) ;
- le traitement des risques (2.3.3.5) ;
- les activités de contrôle (2.3.3.6) ;
- l'information et la communication (2.3.3.7) ;
- le pilotage (2.3.3.8).

#### **2.3.3.1. L'environnement interne**

L'environnement interne est le reflet du style d'une organisation ; il révèle la sensibilisation aux risques des personnes qui la composent et constitue ainsi le fondement structurel sur lequel peuvent s'appuyer tous les autres éléments du dispositif de gestion des risques. Il comprend notamment les éléments suivants :

- la culture du risque de l'entité, qui doit être comprise du personnel et reflétée dans les politiques, communications et actions de la direction ;
- l'appétence pour le risque de l'entité, soit le niveau de risque que l'entité est prête à accepter pour atteindre ses objectifs (estimable quantitativement ou qualitativement) ;
- la surveillance exercée par la haute direction (esprit, indépendance et expérience, degré d'implication) ;
- l'intégrité et les valeurs éthiques, notamment par le biais d'un code de conduite, l'existence de sanctions, la communication, les incitations) ;
- l'organisation (structure cohérente), le mode de délégation des pouvoirs et responsabilités et les compétences du personnel (adaptées au cahier des charges) ;
- la politique du personnel (pratiques en matière d'engagement, de formation, de rémunération et de promotion).

#### **2.3.3.2. La définition des objectifs**

Les objectifs sont définis à un niveau stratégique et constituent la base sur laquelle se fondent les opérations de niveau inférieur.

Pour être en mesure d'identifier les opportunités et menaces, de les évaluer et d'y répondre efficacement, il est nécessaire que les objectifs aient été fixés. Ces objectifs peuvent être classés en objectifs stratégiques, opérationnels, de conformité et relatifs aux rapports d'information financière, comme décrit au paragraphe 2.3.1.

### 2.3.3.3. L'identification des événements

Il s'agit, sous la responsabilité de la direction de l'entité, d'identifier les événements potentiels qui affecteront l'organisation s'ils se réalisent, en distinguant les événements positifs (opportunités) des événements pouvant nuire sérieusement à la capacité de l'entité à atteindre ses objectifs et mettre en œuvre avec succès sa stratégie (risques).

Les risques doivent par la suite faire l'objet d'une évaluation et de l'élaboration d'une solution alors que les opportunités sont à intégrer à la stratégie et aux objectifs. À noter qu'un même événement peut être à la fois un risque et une opportunité.

Pour identifier les divers événements, la direction de l'entité doit examiner à l'échelle globale de l'organisation les différents facteurs :

- a) les facteurs exogènes, soit des changements dans l'environnement :
  - économiques (prix, coût, barrières) ;
  - environnementaux ;
  - politiques (lois, règlements) ;
  - sociaux (démographie, terrorisme, migrations) ;
  - technologiques (Internet).
- b) les facteurs endogènes, soit des choix de la direction de l'entité quant au fonctionnement :
  - des infrastructures (disponibilité, capacité) ;
  - du personnel (compétence, fraude, sécurité) ;
  - des processus (conception, exécution) ;
  - de la technologie (système informatique).

L'identification des événements peut se faire par des méthodes rétrospectives (basées sur la revue de rapports, des historiques, p. ex.) et/ou prospectives (évolution démographique, conditions de marché, p. ex.). Les méthodes les plus fréquemment utilisées, en raison de leur simplicité de mise en œuvre, sont :

- *Catalogue d'événements* — consiste à utiliser une liste d'événements potentiels communs au secteur d'activité de l'entité ou à ses processus ;
- *Groupe de travail, brainstorming, entretiens* — consistent à exploiter l'expérience de tous lors de discussions structurées ;
- *Questionnaires et enquêtes* — consistent à adresser des questions (ouvertes, semi-ouvertes ou fermées) à une sélection de personnes.

### 2.3.3.4. L'évaluation des risques

L'évaluation des risques consiste à déterminer dans quelle mesure les événements potentiels identifiés sont susceptibles d'avoir un impact sur la réalisation des objectifs, en évaluant d'une part la **probabilité d'occurrence**,

d'autre part l'**impact** (quantitatif ou qualitatif) de réalisation de ces événements (pris individuellement ou regroupés par catégorie).

L'évaluation doit porter dans un premier temps sur les **risques inhérents** aux activités et à la situation de l'organisation (évaluation brute). Dans un deuxième temps, suite à l'élaboration des réponses aux risques, la validité des mesures réduisant les risques et les **risques résiduels** devront être également estimés (évaluation nette).

### **Méthodes d'évaluation**

Les techniques d'évaluation sont soit qualitatives, soit quantitatives. La méthode sur laquelle se base la Cour des comptes est celle qui consiste à estimer séparément la probabilité d'occurrence et l'ampleur potentielle des dommages causés par un événement en recourant à une échelle que l'entité aura définie. Afin d'évaluer le risque, une méthode consiste à multiplier les deux estimations entre elles (espérance mathématique).

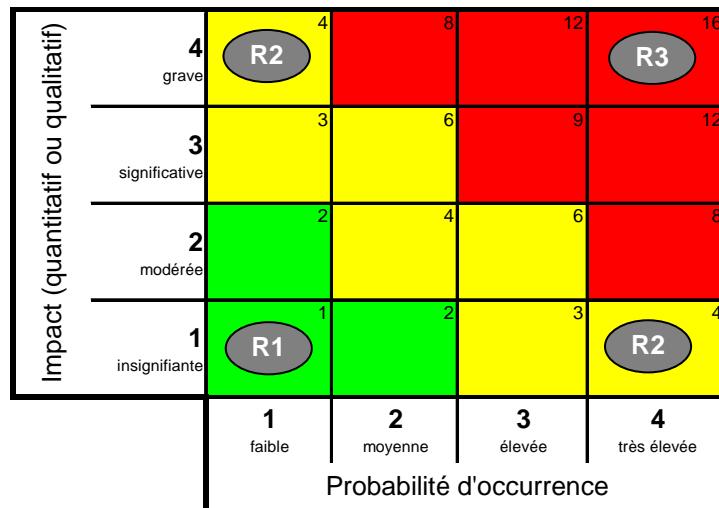
### **Conditions d'une bonne évaluation**

Les conditions d'une bonne évaluation sont les suivantes :

- La période considérée doit être cohérente avec celle fixée pour la réalisation des objectifs ;
- La fiabilité des données doit être assurée ;
- L'évaluation doit se faire de manière groupée en cas d'événements corrélés ;
- Le personnel impliqué doit comprendre la signification du système de notation ou de l'échelle utilisée ; une qualification des échelles utilisées est requise (p. ex. « peu probable » : une occurrence tous les trois ans) ; le nombre des classes d'impact et de probabilité est défini par les directives en vigueur ou, à défaut, par les responsables du processus de gestion des risques ;
- Tous les responsables, quel que soit leur niveau, doivent évaluer les événements susceptibles d'affecter leur domaine d'activité et en informer les hauts responsables ;
- L'évaluation doit être effectuée dans les différentes unités puis consolidée afin d'assurer une vision globale des risques à la direction de l'entité.

À la fin du processus d'évaluation des risques, les résultats de l'analyse des risques sont généralement représentés sous la forme d'une **cartographie**.

**Exemple de cartographie des risques inhérents (évaluation brute)**



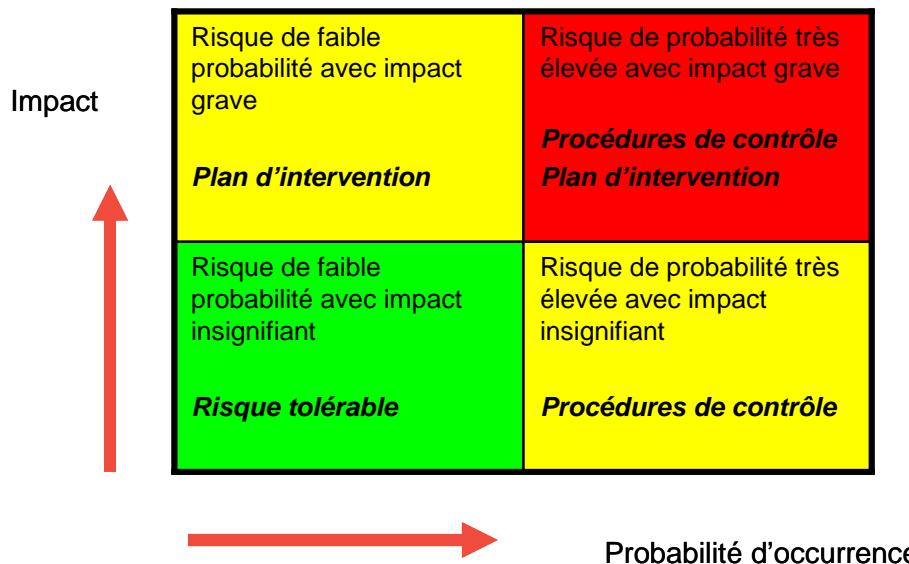
Source : Adapté du *Guide concernant le système de contrôle interne des processus avec incidences financières dans l'administration fédérale*, p.21

### 2.3.3.5. Le traitement des risques

Une fois les risques évalués, la direction doit déterminer quelles solutions appliquer à chacun des risques, l'objectif étant :

- d'exclure toute faiblesse majeure (concentration sur les risques élevés) ;
- de s'assurer que tous les risques ont été ramenés à des paramètres acceptables dans les limites du degré d'aversion au risque de l'entité ;
- de profiter des opportunités (optimisation).

Les principes de base de réponses aux risques sont les suivants :



Ainsi, pour répondre aux risques, la direction se trouve face aux solutions suivantes :

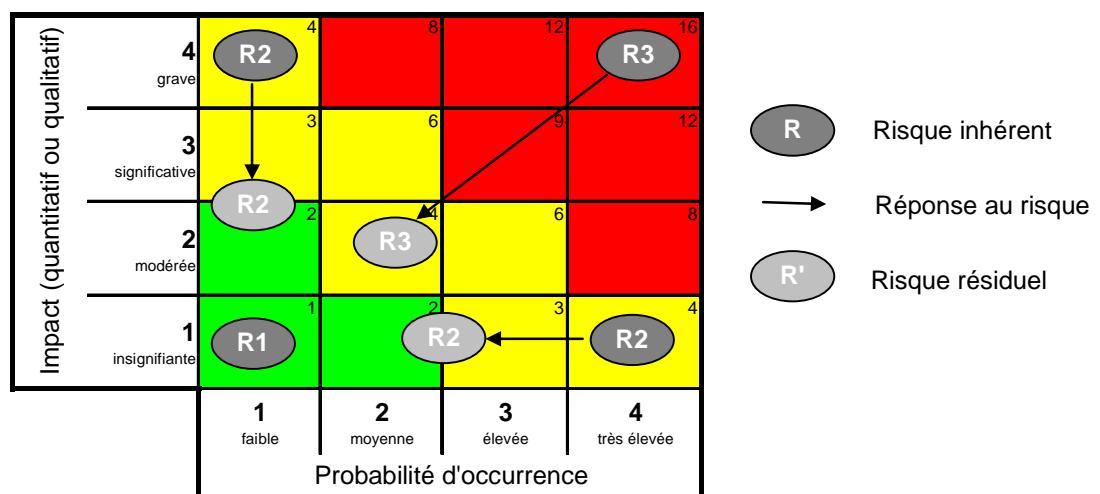
Principe	Réponses possibles aux risques
Plan d'intervention ou procédures de contrôle	Évitement ou fin de l'activité risquée : Suppression de l'activité risquée.
	Réduction du risque : Réduction de la probabilité ou de l'étendue des dommages (ou des deux) par des décisions de gestion, en passant notamment par le système de contrôle interne.
Tolérance du risque	Transfert du risque : Réduction de la probabilité ou de l'étendue des dommages (ou des deux) en transférant une partie du risque (exemple : par une assurance, une externalisation, une couverture).

En se référant à la cartographie des risques représentée ci-dessus :

- R1** Pour les risques dont l'évaluation brute est qualifiée de **faible** (vert), il n'est pas efficient de prendre des mesures particulières ou de procéder à des contrôles ;
- R2** Pour les risques dont l'évaluation brute est qualifiée de **moyenne** (jaune), des mesures ou/et des contrôles s'imposent ; une analyse coût-utilité peut cependant justifier l'adoption de procédures simplifiées (par exemple : contrôle par sondage au lieu d'un contrôle intégral).
- R3** Pour les risques dont l'évaluation brute est qualifiée d'**élevée** (rouge), la formulation et la mise en place de mesures et de contrôles est indispensable.

Il convient de considérer l'effet des différentes solutions en termes de probabilité et d'impact ainsi qu'en termes de rapport coût/bénéfice de la solution (**évaluation du risque résiduel**). Le choix doit porter sur la solution ramenant le risque résiduel en dessous du seuil de tolérance au risque défini par la direction.

**Exemple de cartographie des risques résiduels  
(évaluation nette, après mise en place des réponses)**



Source : Adapté du *Guide concernant le système de contrôle interne des processus avec incidences financières dans l'administration fédérale*, p.21

Les risques (et opportunités) doivent être appréhendés de manière transversale/agrégée de manière à s'assurer que le risque résiduel global corresponde à l'appétence de l'organisation pour le risque.

### 2.3.3.6. Les activités de contrôle

Les activités de contrôle sont constituées des politiques et procédures permettant d'assurer que les réponses aux risques adoptées par la direction sont effectivement et efficacement mises en place. Elles sont présentes à tout niveau et dans toute fonction de l'organisation. Elles font partie du système de contrôle interne de l'entité.

### 2.3.3.7. L'information et la communication

La capacité des responsables à prendre les décisions appropriées est conditionnée par la qualité de l'information ; il s'agit donc qu'elle soit adéquate, disponible en temps opportun, à jour, exacte et accessible.

En outre, une communication efficace doit circuler de manière ascendante, transversale, et descendante dans l'organisation, dans toutes ses composantes et dans l'ensemble de sa structure, pour que chacun dispose à temps et de manière appropriée des règles nécessaires à l'exercice de son rôle et des responsabilités en matière de gestion des risques.

- La **direction** doit communiquer de manière ciblée et spécifique au sujet de sa gestion des risques, notamment sur les éléments suivants : les objectifs de l'entité, l'importance de la gestion des risques pour l'entité et son appétence au risque, le langage commun d'évaluation et les rôles et responsabilités du personnel.
- Le **personnel** doit également disposer de canaux pour communiquer les informations relatives aux risques à la direction par les canaux de communication habituels ou alternatifs (par exemple : ligne téléphonique).

### 2.3.3.8. Le pilotage

Le dispositif de gestion des risques doit faire l'objet d'un pilotage qui repose sur l'évaluation de l'existence et du bon fonctionnement de ses éléments. Comme le dispositif évolue dans le temps (risques, solutions adéquates, activités de contrôle efficaces), il est primordial de déterminer si le fonctionnement du dispositif reste efficace face aux changements.

Le pilotage peut se faire par :

- a) un **dispositif continu**, qui découle d'activités de gestion courantes réalisées par les responsables opérationnels ou fonctionnels (par exemple : revue des rapports internes par la direction) ;
- b) des **évaluations spécifiques** (auto-évaluations ou évaluations par des tiers), portant sur la pertinence du processus et le fonctionnement effectif ainsi que sur la documentation disponible, adaptées à la taille et à la complexité de l'entité (organigrammes, cahiers des charges, manuels de politiques et de procédures, diagrammes de flux, matrices de risques et contrôles) ; l'étendue et la fréquence de ces évaluations dépendent du niveau des risques.

## CHAPITRE 3

# LA METHODOLOGIE DES MISSIONS DE VERIFICATION DE L'EVALUATION DE LA GESTION DES RISQUES

Le présent chapitre a pour objectif de présenter :

- d'une part de manière synthétique la méthodologie de la Cour développée en détail dans le *Manuel de méthodologie générale de la Cour des comptes du Canton de Vaud* ;
- d'autre part son application spécifique aux missions de vérification de l'évaluation de la gestion des risques ; cette application est mise en évidence dans des encadrés.

La Cour des comptes a en outre développé un outil de vérification spécifique aux missions de vérification de l'évaluation de la gestion des risques qui est présenté en annexe.

Avant de se pencher sur la méthodologie, il est important de rappeler que la Cour des comptes a pour mission de vérifier l'évaluation de la gestion des risques des entités incluses dans son champ de contrôle, sous l'angle de la forme et non du contenu. Elle n'est en aucun cas responsable d'évaluer le contenu de l'évaluation des risques mais elle s'assure néanmoins de la cohérence des mesures prises en la matière. Elle évalue ainsi le processus de gestion des risques.

### 3.1. Aperçu de la méthodologie

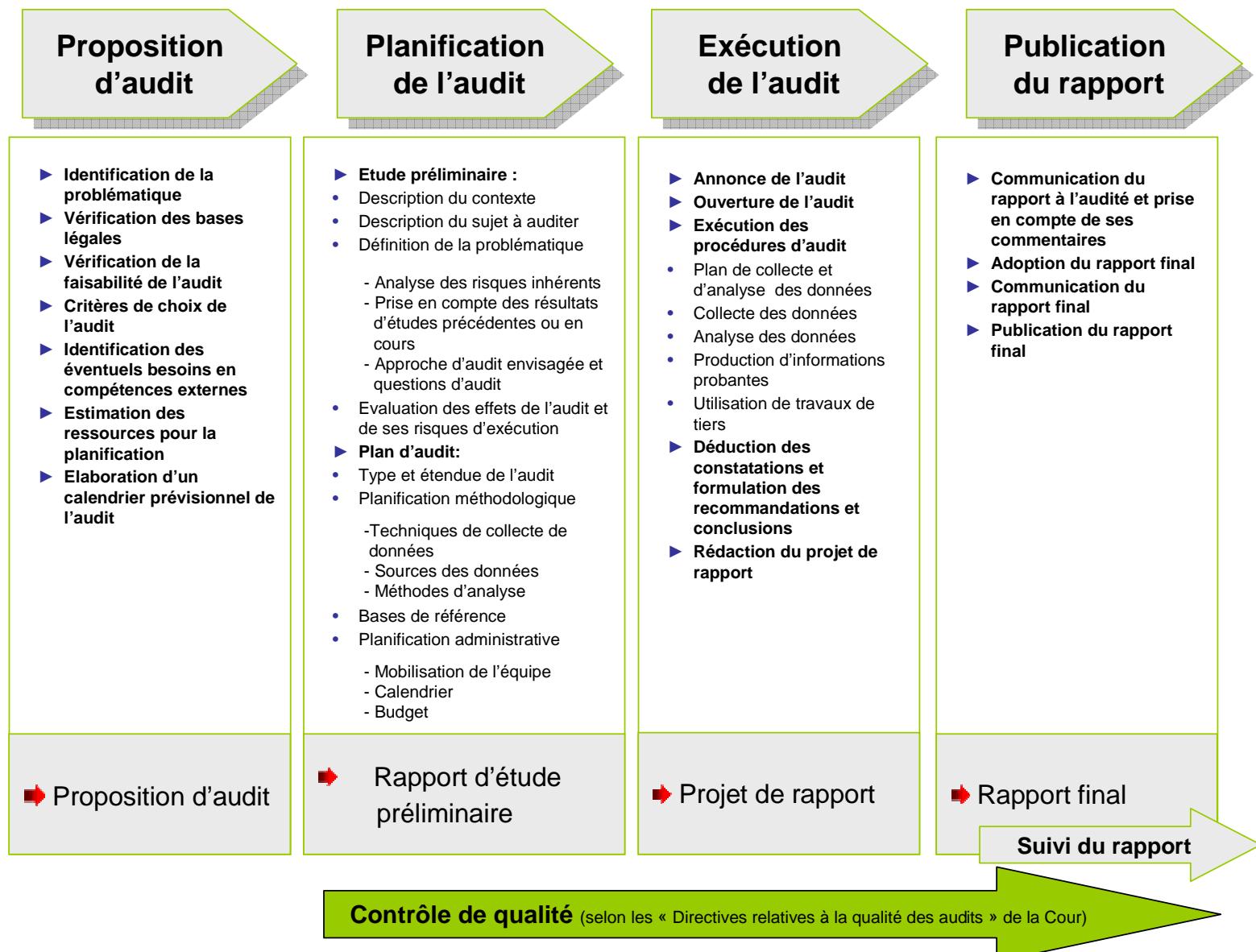
Afin de remplir ses missions, la Cour établit un plan stratégique à trois ans qui définit sa vision à moyen terme. Pour assurer la mise en œuvre de ce plan, elle identifie de manière permanente des domaines de contrôles potentiels et tient à jour la liste des thèmes possibles. Ce processus sert de base à l'élaboration du plan de travail annuel, dans lequel la Cour des comptes fixe les priorités qu'elle entend respecter en termes de types de contrôle, de thèmes généraux et/ou de domaines concernés, d'entités concernées et en fonction de l'évaluation des risques.

Dès lors qu'un thème d'audit a été identifié par la Cour, ce thème est étudié puis, si cela s'avère approprié, planifié et exécuté. Ainsi, tout audit de la Cour se déroule en **quatre phases** bien distinctes :

- La phase de proposition du thème de l'audit (chapitre 3.2) ;
- La phase de planification de l'audit, qui doit servir à déterminer si l'audit est réaliste, réalisable et susceptible d'être utile et débouche sur la production d'un rapport d'étude préliminaire (chapitre 3.3) ;
- La phase d'exécution de l'audit, qui se termine par le projet de rapport (chapitre 3.3) ;
- La phase de publication du rapport final (chapitre 3.4).

Dans la pratique, il s'agit d'un processus continu, à savoir que les quatre phases s'enchaînent les unes aux autres sans interruption.

Le suivi du rapport ne fait volontairement pas l'objet d'une phase formelle. En effet, la loi sur la Cour des comptes ne le prévoit pas, considérant que le suivi des recommandations relève de la compétence des destinataires du rapport, et non de celle de la Cour des comptes. Toutefois, dans le but d'évaluer ses propres résultats, la Cour s'informe auprès de l'entité auditee, dans un délai de six mois à une année après la publication du rapport, des effets de ses recommandations (voir chapitre 3.6).



### 3.2. La phase de proposition du thème de l'audit

La première phase de tout audit consiste en l'élaboration d'une proposition d'audit qui a pour objectif de déterminer si un thème évoqué par un membre de la Cour ou de son personnel est susceptible de faire l'objet d'un audit.

En préambule, il est utile de rappeler qu'en dehors des cas d'attribution d'un mandat du Grand Conseil, la Cour des comptes est seule juge des priorités à accorder lors la sélection des thèmes d'audit, selon la pertinence des critères de choix retenus et les ressources disponibles. Les thèmes d'audit ainsi sélectionnés peuvent alors résulter d'une auto-saisine, d'une proposition du Conseil d'État ou d'un signalement. En cas de mandat attribué à la Cour des comptes par le Grand Conseil, cette première phase de « proposition d'audit » ne s'applique pas et l'audit débute avec la phase de planification directement.

L'étape de proposition du thème de l'audit est interne à la Cour et ne peut prévoir que des contacts limités avec les responsables des entités concernées. Le processus consiste en l'examen des éléments suivants:

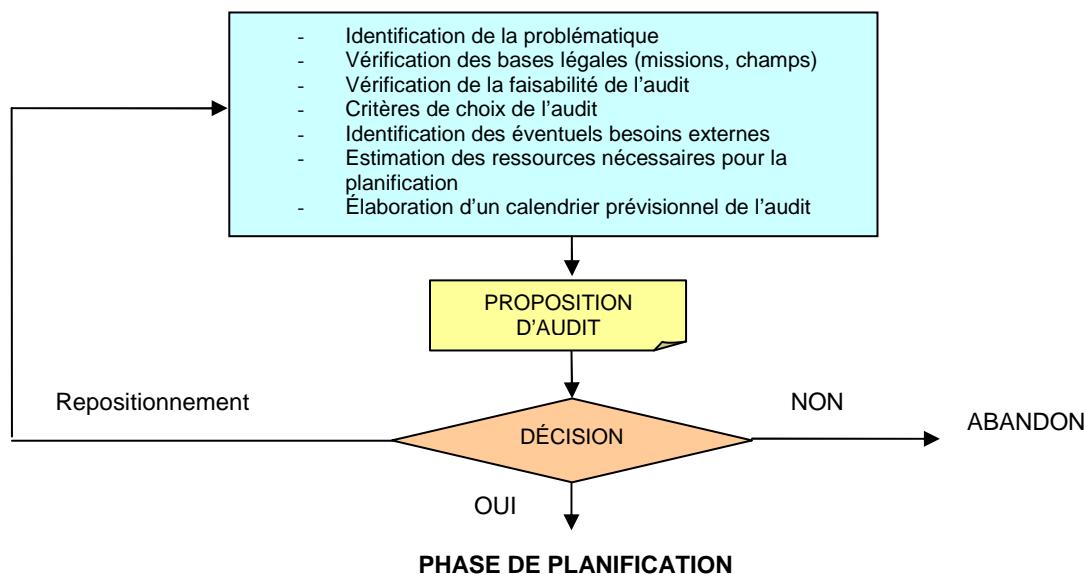
- L'identification de la problématique ;
- Les bases légales (missions et champ de contrôle de la Cour) ;
- La faisabilité de l'audit ;
- Les critères de choix des audits ;
- Les éventuels besoins externes identifiés à ce stade pour la phase de réalisation de l'étude préliminaire ;
- Les ressources nécessaires pour la phase de planification ;
- Le calendrier prévisionnel.

La phase de proposition d'un thème d'audit débouche sur une **proposition d'audit** écrite soumise à la Cour, qui décide sur cette base si une étude préliminaire doit être effectuée.

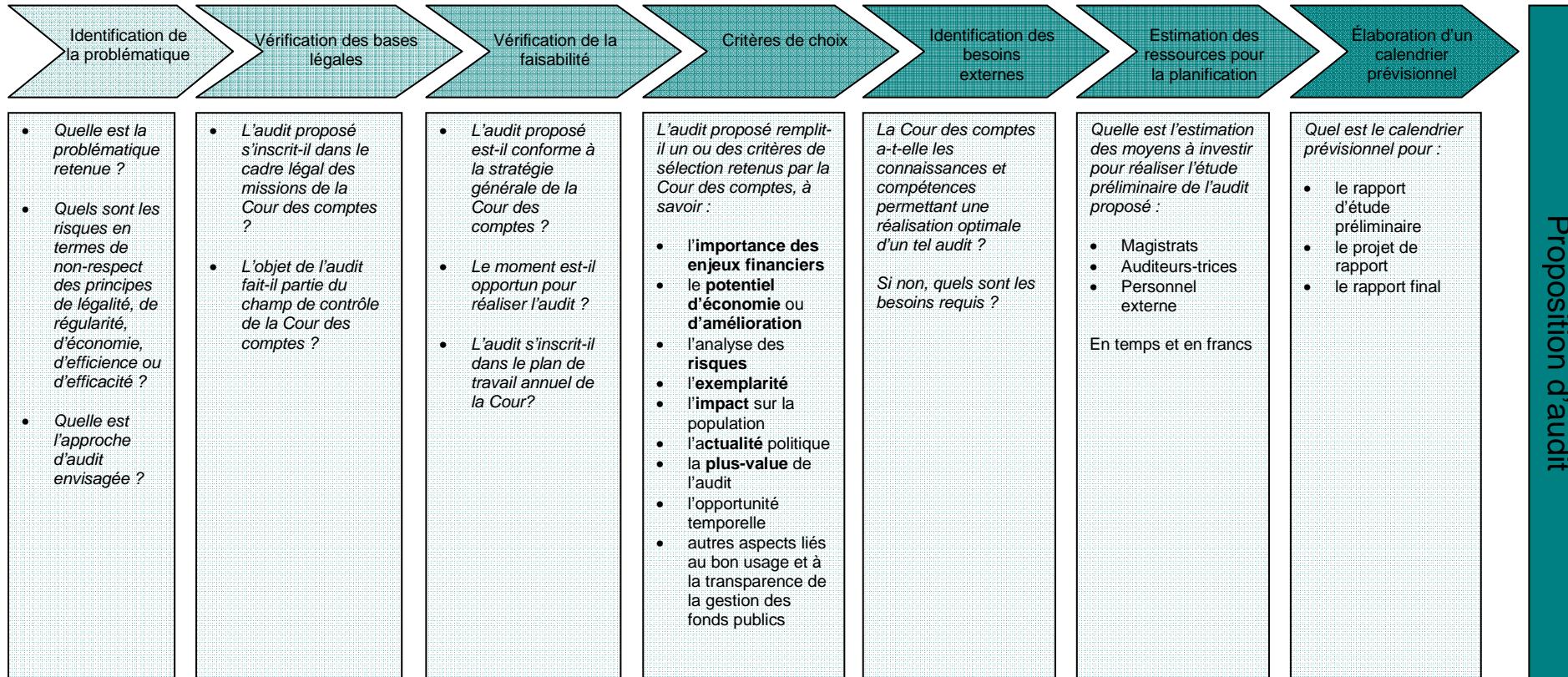
La phase de proposition de l'audit est développée de manière détaillée au chapitre 3 du volume *Méthodologie générale de la Cour des comptes du Canton de Vaud*, le modèle de proposition d'audit figurant en Annexe 1 de ce même volume.

Ces différents éléments sont reflétés de manière résumée dans l'illustration et le tableau ci-après :

## Représentation graphique de la phase de proposition du thème de l'audit



# La phase de proposition du thème de l'audit



### 3.3. La phase de planification de l'audit

La phase de planification de l'audit débute dès que la proposition d'audit a été acceptée par la Cour et constitue la phase préparatoire de l'audit. Elle nécessite une prise de contacts avec les parties concernées par l'audit, en particulier l'entité à auditer et, le cas échéant, certains experts.

La phase de planification comprend trois étapes :

- 3.3.1 l'étude préliminaire ;
- 3.3.2 le plan d'audit ;
- 3.3.3 le rapport préliminaire.

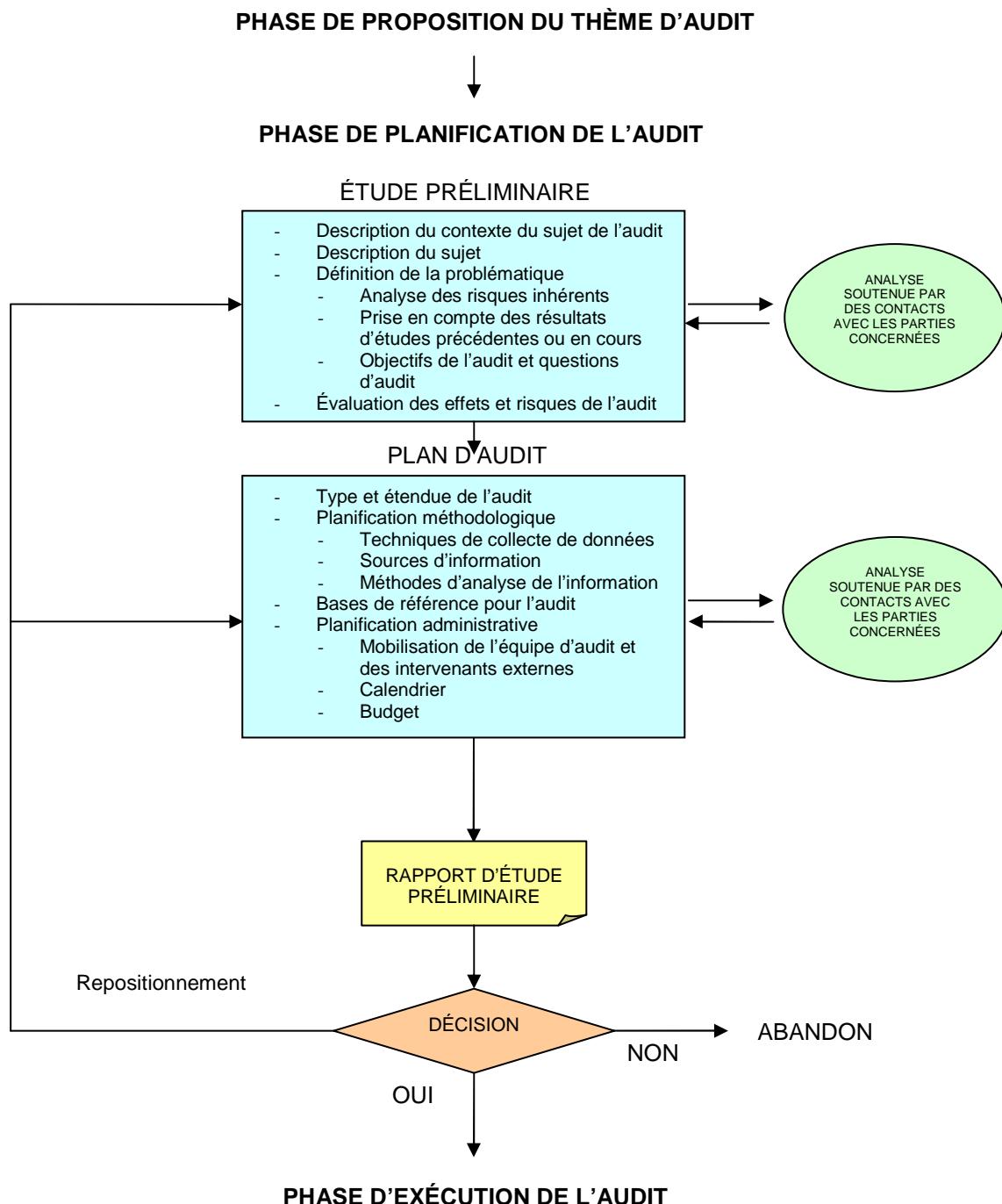
Elle débouche sur la mise au point d'un rapport d'étude préliminaire<sup>17</sup>, qui est soumis à la Cour en séance plénière. La Cour décide sur cette base d'exécuter ou non l'audit envisagé.

Les différentes étapes de la phase de planification sont reflétées dans le schéma ci-dessous. Une description détaillée de chacune d'elles figure au chapitre 4 du volume *Méthodologie générale de la Cour des comptes du Canton de Vaud*.

---

17. La description du contenu du rapport préliminaire peut-être consultée au chapitre 4, paragraphe 4.3. du *Manuel de la méthodologie générale de la Cour des comptes du Canton de Vaud*.

## Représentation graphique de la phase de planification de l'audit



### 3.3.1. L'étude préliminaire

L'étude préliminaire consiste à préciser le contenu de l'audit. Elle consiste en trois éléments principaux. Sa description détaillée figure au chapitre 4, paragraphe 4.1. du *Manuel de méthodologie générale*.

#### La description du contexte et l'étude du sujet d'audit

Il est nécessaire pour les auditeurs de décrire et de comprendre

- les contextes juridique, politique et économique dans lesquels évolue l'entité à auditer ;
- le fonctionnement de l'entité à auditer.

Une connaissance approfondie du sujet de l'audit et de son environnement doit être acquise afin que l'équipe d'audit soit mieux à même de vérifier les éléments du processus de gestion des risques adopté par l'audité.

#### La définition de la problématique

La définition de la problématique consiste à délimiter les frontières de l'audit, à savoir :

- les objectifs de l'audit
- les questions d'audit

Sur la base de l'estimation des risques inhérents à l'entité et après avoir pris connaissance des résultats d'études précédentes et d'études en cours, les auditeurs dégagent les **objectifs principaux de l'audit**, qui constituent le cadre de référence des auditeurs tout au long du processus d'audit. Ces objectifs sont traduits en questions d'audit.

Les objectifs d'une mission de vérification de l'évaluation de la gestion des risques sont identiques pour toute mission de ce type. Il s'agit d'examiner le processus suivi par l'audité pour sa gestion des risques, par rapport aux bonnes pratiques en la matière, en particulier les étapes prévues par la méthodologie COSO II.

Dans une mission de ce type, les questions d'audit sont relatives à l'évaluation des éléments du modèle de référence (chapitre 2.3). Elles sont identiques pour toute mission de ce type et sont décrites dans la check-list pour la vérification de l'évaluation de la gestion des risques (Annexe 1), qui sert d'outil de vérification à la Cour.

## Évaluation des effets de l'audit et de ses risques d'exécution

Avant de prendre la décision d'exécuter la mission, les effets de l'audit et les risques de bonne exécution doivent être examinés (par exemple, moment inopportun, retards dans l'exécution, inadéquation des ressources, décision politique ayant une influence sur le thème de l'audit).

### 3.3.2. Le plan d'audit

Pour une description détaillée des phases du plan d'audit, le lecteur se réfère au *Manuel de la méthodologie générale de la Cour des comptes*, chapitre 4, paragraphe 4.2.

Le **plan d'audit** vérifie si l'audit est réalisable en se référant de manière plus précise aux **moyens** utilisés pour atteindre les objectifs. L'impossibilité de définir des moyens d'atteindre les objectifs constitue une remise en question de la faisabilité de l'audit considéré.

Le plan d'audit comprend les éléments suivants :

#### Le type et l'étendue de l'audit

L'auditeur doit définir le type d'audit qui sera effectué parmi les différents types d'audit synthétisés au paragraphe 1.2.4.

Le type d'audit est, dans le cadre de ce manuel, un audit de la vérification de l'évaluation de la gestion des risques.

Toutefois, une mission de vérification de l'évaluation de la gestion des risques comporte également des éléments de type conformité, puisqu'elle consiste à vérifier que le processus de gestion des risques suivi par l'audité est conforme aux bonnes pratiques. Ces bonnes pratiques peuvent être déduites du modèle COSO II adapté au secteur public (voir chapitre 2.3.). La mission s'approche aussi de la vérification des résultats, dans le sens où l'évaluation porte sur l'économie, l'efficience et l'efficacité de la gestion des risques.

En outre, il s'agit de limiter si nécessaire l'étendue de l'audit (lieux, période, documents, processus, etc. à auditer).

La mission de vérification de l'évaluation de la gestion des risques porte sur l'ensemble des catégories de risques liées aux catégories d'objectifs définies dans le modèle de gestion des risques (voir 2.3.1.), ainsi qu'aux risques spécifiques que sont le risque de contrôle, le risque d'irrégularités, de fraude et de corruption, et le risque d'image (voir 2.1.2, 3<sup>e</sup> paragraphe). Cependant, en raison des travaux qu'effectuent le Contrôle Cantonal des Finances ou le réviseur externe sur le système de contrôle interne relatif à l'établissement des comptes (au terme de la NAS 890), la Cour détermine au cas par cas le niveau d'analyse qu'elle souhaite mener.

## La planification méthodologique

La planification méthodologique a pour but de concrétiser l'étude de la problématique dans la description des étapes successives de la démarche d'audit. Pour chacune des étapes, il s'agit d'identifier les sources d'information, ainsi que les techniques de collecte et d'analyse des données.

Pour les missions de vérification de l'évaluation de la gestion des risques, la Cour prévoit généralement de récolter et d'analyser les données de la manière suivante :

- Des informations préliminaires sont récoltées au moyen d'une **check-list** développée par la Cour (voir annexe). La check-list est exposée et transmise à l'audité lors de la séance de démarrage de l'audit. Il lui est demandé de compléter la check-list et de remettre à l'équipe d'audit les documents étayant les réponses données (par ex. : politique de gestion des risques de l'entité, catalogue des risques, résultat de l'évaluation des risques, etc.). Un délai de réponse est convenu entre l'audité et l'équipe d'audit. Selon les circonstances, l'équipe d'audit complète la check-list avec l'audité.
- Une fois la check-list complétée et les documents justificatifs reçus, l'équipe d'audit en fait une première analyse puis mène sur cette base des **entretiens** avec le responsable de l'entité auditee, le responsable de la gestion des risques (si différent) et un certain nombre de personnes participant au processus de gestion des risques (par ex. : chefs de service) afin de corroborer les informations obtenues et d'obtenir les **éléments probants** manquants (voir chapitre 3.4.3.).
- Les informations récoltées sont finalement évaluées par **comparaison avec le modèle** de processus de gestion des risques représentant les bonnes pratiques en la matière qui est présenté au chapitre 2.3. de ce manuel.
- Les constatations et recommandations sont discutées avec l'audité.

## Les bases de référence pour l'audit

Les bases de référence de l'audit sont des normes pertinentes, raisonnables et réalisables selon lesquelles les aspects d'économie, d'efficience et d'efficacité peuvent être évalués. Les constatations de la vérification des résultats naissent de la comparaison entre les critères et les faits.

Le modèle de processus de gestion des risques utilisé par la Cour (voir chapitre 2.3.) a été établi sur la base du modèle COSO II, modèle par ailleurs repris dans les *Lignes directrices pour le contrôle interne — Informations complémentaires sur la gestion des risques des entités* publiées par INTOSAI.

## La planification administrative

La planification administrative consiste à organiser l'audit en termes de ressources humaines et financières. Il s'agit de définir la composition de l'équipe d'audit (y. c. les mandataires externes), le calendrier et le budget.

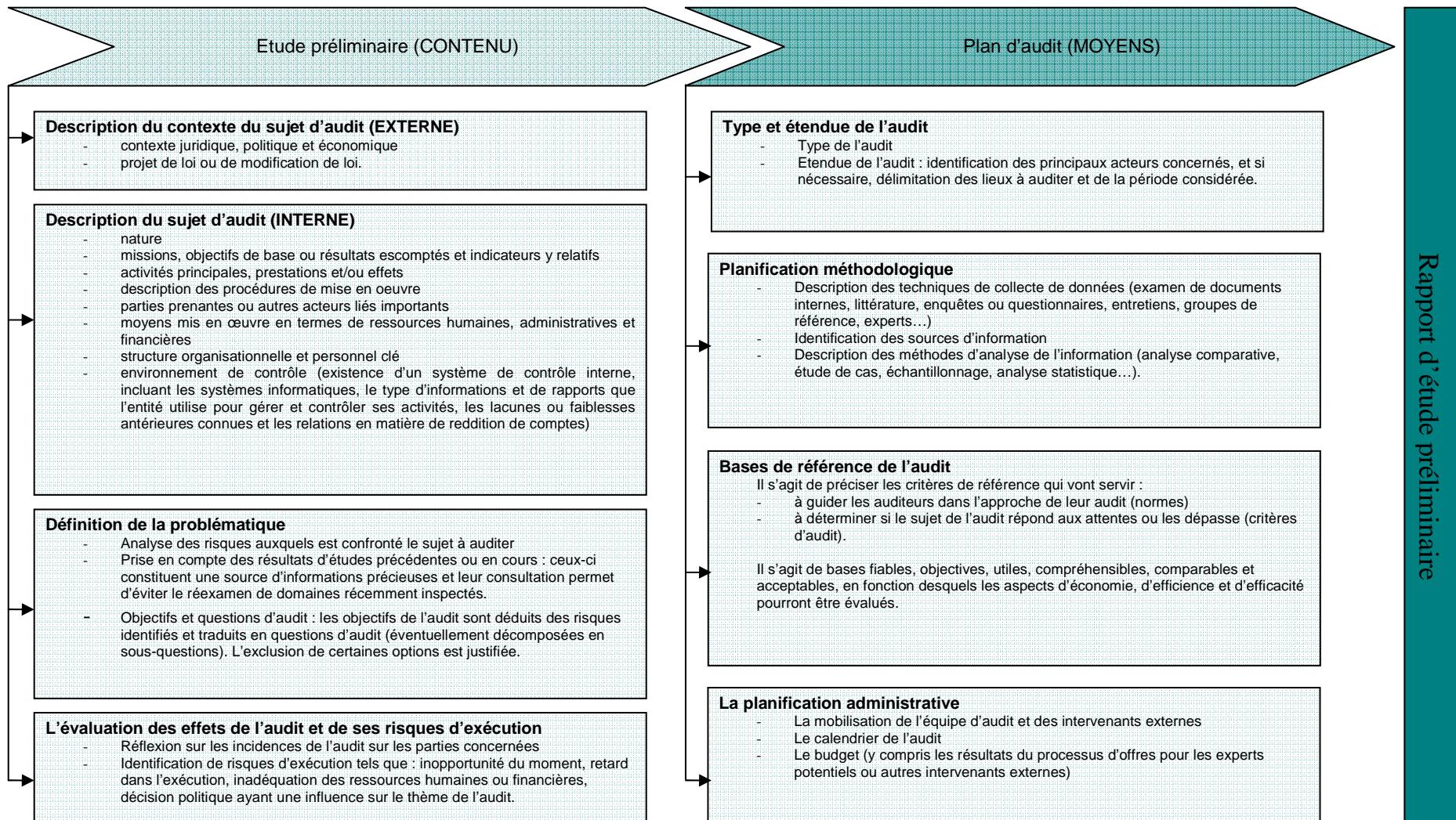
### 3.3.3. Le rapport d'étude préliminaire

La phase de planification débouche sur la mise au point d'un rapport d'étude préliminaire, qui sera établi dans tous les cas et soumis à la Cour, laquelle peut demander d'en affiner ou d'en modifier certains points avant de décider sur cette base d'exécuter ou non l'audit.

Le contenu du rapport d'étude préliminaire est décrit dans le *Manuel de méthodologie générale de la Cour des comptes*, chapitre 4, paragraphe 4.3.

La phase de planification est reflétée de manière résumée dans l'illustration ci-dessous :

# La phase de planification de l'audit



### 3.4. La phase d'exécution de l'audit

La phase d'exécution de l'audit comprend les étapes suivantes :

- 3.4.1. L'annonce de l'audit ;
- 3.4.2. La séance d'ouverture de l'audit ;
- 3.4.3. L'exécution des procédures d'audit ;
- 3.4.4. La rédaction des constatations et la formulation des recommandations (résultats de l'audit) ;
- 3.4.5. Le projet de rapport.

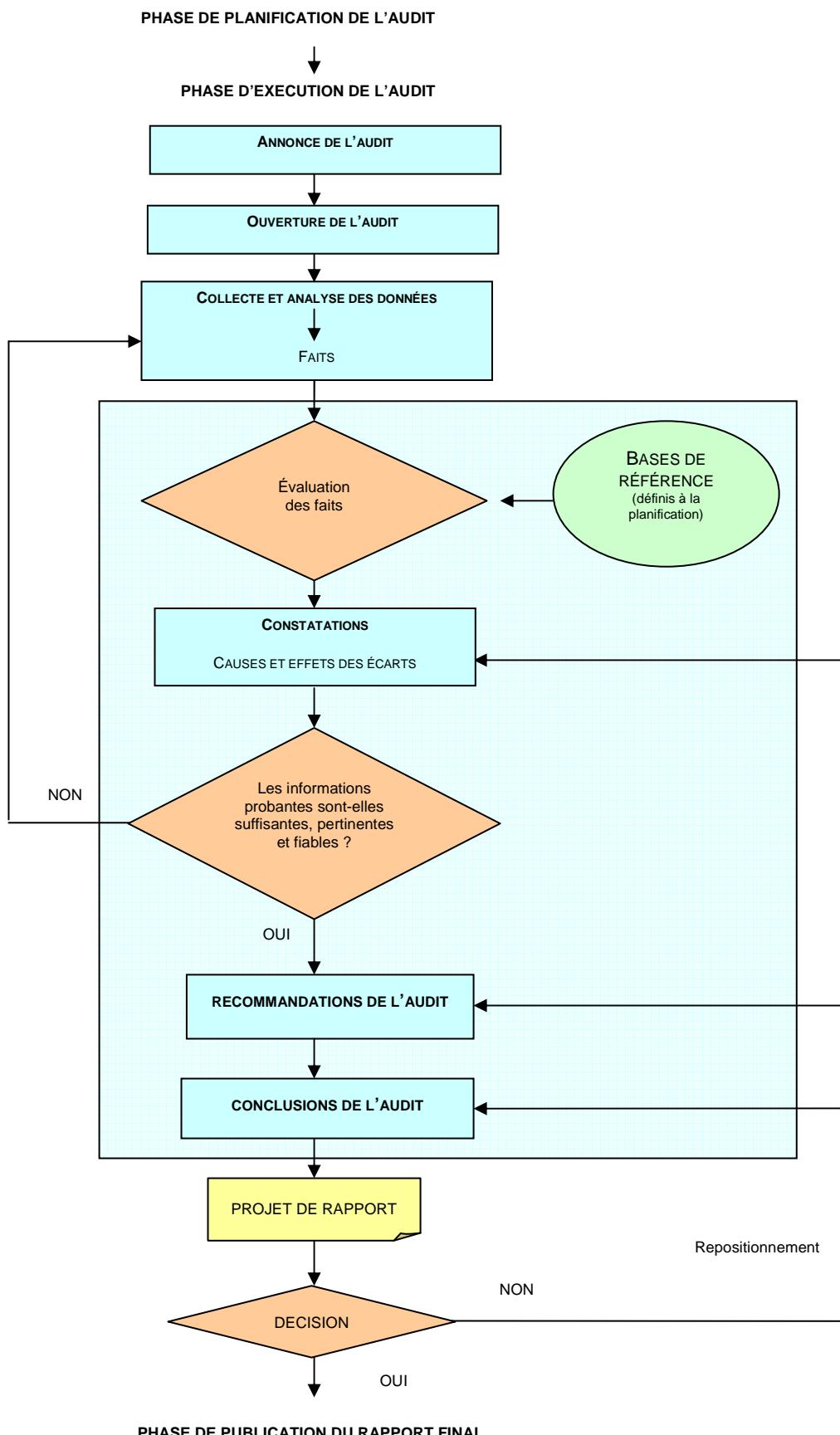
L'exécution d'un audit est un processus d'analyse et de communication. Dans la partie analytique, les données sont recueillies, interprétées et analysées. La partie communication se réfère quant à elle au processus d'interaction qui se met en place entre l'auditeur et l'audité.

L'équipe d'audit veille à respecter scrupuleusement tout au long de l'audit le *Code de déontologie*, le manuel d'assurance qualité et la méthodologie de la Cour, basés sur les normes de contrôle de l'INTOSAI.

L'audit doit être réalisé conformément aux décisions prises dans le cadre de l'adoption par la Cour du rapport d'étude préliminaire. Néanmoins, la Cour doit rester ouverte et flexible par rapport à des modifications souhaitables du plan de travail en cours d'audit (tout changement de direction et élargissement de la mission d'audit doit être justifié et estimé en termes de consommation de ressources par la Cour elle-même).

Le détail du processus d'exécution des procédures d'audit est explicité dans le *Manuel de méthodologie générale de la Cour des comptes*, chapitre 5.

La phase d'exécution de l'audit est schématisée dans l'illustration suivante :



### **3.4.1. L'annonce de l'audit**

Une fois le rapport d'étude préliminaire adopté par la Cour, la Cour annonce officiellement par écrit le début de l'audit simultanément au Conseil d'État, au Grand Conseil et au Contrôle cantonal des finances, ainsi qu'aux responsables de l'entité auditee (art. 2 et 24ss de la LCComptes). L'audit reste confidentiel jusqu'à la publication du rapport final.

### **3.4.2. La séance d'ouverture de l'audit**

L'équipe d'audit pouvant être confrontée à des situations très diverses, il importe qu'elle mette en place **un processus constructif d'interaction** avec l'entité auditee. Afin de permettre l'ouverture avec l'audité d'un dialogue basé sur la confiance réciproque, une rencontre avec ce dernier est organisée suite à l'annonce de l'audit pour présenter l'équipe d'audit, exposer en quoi consistera la mission et planifier son déroulement avec l'audité.

Il s'agit plus particulièrement de présenter ce que la Cour entend par « gestion des risques » et ce que l'équipe d'audit entend vérifier, soit le processus suivi et non l'évaluation en elle-même.

### **3.4.3. L'exécution des procédures d'audit**

L'exécution proprement dite de l'audit consiste à collecter et à analyser des données pouvant être utilisées pour étayer les constatations effectuées et élaborer les recommandations de la Cour.

#### **La collecte et l'analyse des données**

L'équipe d'audit commence l'exécution de l'audit par l'élaboration du **plan de collecte et d'analyse des données**.

Les techniques de collecte et d'analyse des données ainsi que les sources d'informations ont été décrites au niveau du plan d'audit (3.3.2). Le terme d'analyse de données est généralement utilisé pour désigner à la fois la compilation (encodage et présentation sous forme de tableaux), et l'analyse de données proprement dite.

L'analyse des données doit être conçue et orientée par les auditeurs de manière à :

- atteindre les objectifs de l'audit ;
- permettre la comparaison des informations récoltées avec les critères de référence de l'audit.

## La production d'informations probantes suffisantes, pertinentes et fiables

Une fois les données analysées, l'équipe d'audit doit examiner et juger si les informations ainsi disponibles sont **suffisantes, fiables et pertinentes**.

Si les informations disponibles remplissent les critères ci-dessus, elles sont qualifiées d'informations « **probantes** » et font dès lors office de preuve de ce que l'équipe d'audit avance. Elles peuvent alors être utilisées pour étayer une constatation.

La nature et les caractéristiques des informations probantes selon INTOSAI sont décrites en annexe 6 du *Manuel de méthodologie générale de la Cour des comptes*.

Dans un premier temps, l'équipe d'audit analyse la check-list (cf. annexe) complétée préalablement par l'audité. Elle rassemble ensuite les éléments probants adéquats, afin d'étayer les informations de la check-list, soit :

- par l'obtention de documents démontrant l'existence des éléments de la gestion des risques rapportés dans la check-list ;
- par des entretiens complémentaires avec divers intervenants dans le processus de gestion des risques de l'entité afin de corroborer les informations précédemment récoltées.

Des exemples d'éléments probants sont intégrés dans la check-list développée par la Cour et présentée en annexe.

## Le cas de l'utilisation des travaux de tiers

L'équipe d'audit a la possibilité de se fonder sur des travaux réalisés par des tiers, qui peuvent être des auditeurs internes, d'autres organismes de contrôle ou des experts (engagés ou employés par l'audité ou par la Cour). Étant donné que la Cour détient la responsabilité finale des travaux, dans tous les cas, pour pouvoir utiliser les travaux de tiers, l'équipe d'audit doit acquérir l'assurance raisonnable de leur caractère suffisant, pertinent et fiable.

Lorsque les travaux de tiers sont repris dans le rapport d'audit, la source doit être indiquée, avec d'éventuels commentaires sur les conclusions reprises.

### 3.4.4. La rédaction des constatations et la formulation des recommandations

Sur la base de la combinaison des informations probantes rassemblées, l'équipe d'audit dégage des constatations, puis formule, le cas échéant, des recommandations.

Ce chapitre est détaillé au paragraphe 5.4 du *Manuel de méthodologie générale*.

## Les constatations

Les constatations de l'audit résultent de la comparaison objective entre les informations probantes recueillies par les auditeurs (« ce qui est ») avec « ce qui devrait être » selon les critères de référence déterminés dans le rapport préliminaire. Elles répondent aux questions de l'audit.

L'équipe d'audit examine les différentes informations et documents récoltés sur le processus de gestion des risques existant au sein de l'entité et compare ces éléments avec le modèle établi (voir chapitre 2). Cette comparaison doit permettre de constater les faiblesses et les bonnes pratiques existantes dans la gestion des risques de l'entité, en examinant les aspects de configuration, de mise en œuvre et de documentation du processus.

## Les recommandations

Les **recommandations** sont les moyens d'action suggérés par les auditeurs à partir de l'évaluation des constatations observées. Les recommandations indiquent quelles devraient être les améliorations à apporter à la situation, mais ne constituent en aucun cas des plans d'actions détaillés dont l'élaboration relève des responsables opérationnels.

Comme dans la collecte et l'analyse des informations, l'équipe d'audit formule ses recommandations en restant objective et indépendante. Elles doivent être présentées de manière logique et rationnelle, s'appuyer sur des connaissances précises et être constructives, c'est-à-dire :

- leur tonalité et leur contenu sont positifs ;
- elles visent les résultats ou l'amélioration de performance escomptée ;
- elles tiennent compte des coûts ;
- elles ont fait l'objet d'une discussion avec l'entité auditee.

Dans le cadre d'une mission de vérification de l'évaluation de la gestion des risques, ces recommandations ont pour objectif d'améliorer le processus de gestion des risques de l'entité de manière à ce qu'elle suive les bonnes pratiques en la matière.

## Les conclusions

Sur la base du résultat de ses travaux, l'équipe d'audit doit être en mesure de faire des conclusions spécifiques sur les **questions d'audit** examinées, et ainsi de vérifier si les **objectifs de l'audit** ont bien été atteints. Ses appréciations doivent tenir compte de la situation qui prévalait au moment des prises de décision et indiquer clairement dans le rapport l'étendue des informations dont disposait l'entité contrôlée au moment où les décisions ont été prises.

Au terme de son audit de vérification de l'évaluation des risques, l'équipe d'audit peut évaluer le degré de maturité de la gestion des risques de l'organisation et juger s'il est adapté à l'entité. On peut distinguer les cas de figure suivants (voir également « Évaluation globale » à la fin de la check-list) :

Optimisée	L'entité utilise la gestion des risques comme un outil de pilotage stratégique et de mesure de performance.
Intégrée	La gestion des risques est intégrée aux activités opérationnelles. Le <i>reporting</i> et l'allocation des ressources sont ajustés aux résultats de l'analyse des risques. Des ajustements rapides peuvent être effectués lorsque les conditions évoluent.
Établie	L'entité a mis en place une structure de gestion des risques avec des responsabilités claires. Les principes de la gestion des risques sont décrits de manière détaillée et communiqués au sein de l'entité. L'analyse est menée de manière régulière et quantifie les risques opérationnels de manière anticipée. Elle est suivie d'une stratégie de réduction des risques et est documentée. La direction utilise la gestion des risques comme outil d'aide à la décision.
De base	L'entité dispose d'une gestion des risques centralisée, menée sur une base annuelle, mais limitée et non standardisée et peu documentée. Elle fait l'objet d'un <i>reporting</i> minimal. L'objectif poursuivi est de démontrer que l'entité dispose d'un dispositif minimum de gestion des risques (conformité).
Inexistante	Il n'existe pas de gestion des risques.

La Cour admet que la gestion des risques d'une entité est considérée comme acceptable à partir d'une évaluation « Établie ».

### 3.4.5. Le projet de rapport

La phase d'exécution de l'audit débouche sur la mise au point d'un **projet de rapport**. S'il est validé par la Cour, le projet évoluera en rapport final, publié par la Cour selon la procédure décrite au paragraphe 3.5.

Les directives relatives à la documentation consignée dans les dossiers de travail de la Cour sont détaillées dans le *Code de déontologie et Directives relatives à la*

*qualité des audits, chapitre 2, paragraphe 2.4.4.1. (ou le *Manuel de la méthodologie générale*, annexe 7)*

## La qualité du rapport

Conformément aux normes de contrôle et aux lignes directrices sur la vérification des résultats de l'INTOSAI, le rapport doit être :

- *complet* (tous les arguments et informations nécessaires pour une compréhension correcte des faits rapportés) ;
- *objectif* (faits étayés et présentés de façon impartiale) ;
- *exact* ;
- *convaincant* ;
- *clair* (pour s'adresser à un large éventail de destinataires) ;
- *pertinent* (valeur ajoutée aux parties prenantes et diffusion en temps utile) ;
- *concis* (application du principe de l'importance relative) ;
- *constructif* (exclut les critiques inutiles).

Pour plus de détails, le lecteur se réfère au *Manuel de méthodologie générale de la Cour des comptes*, chapitre 5, paragraphe 5.5.1.

## La structure du rapport

La structure du rapport est organisée de manière à mettre en évidence le lien entre les objectifs de l'audit, traduits à travers les questions d'audit, et les conclusions de l'audit, basées sur les constatations de l'audit.. Elle s'articule de la manière suivante :

### 1. La synthèse

La synthèse inclut d'une part, le **résumé de la mission d'audit** et d'autre part, une **liste exhaustive de toutes les constatations et les recommandations**.

Rédigé en dernier lieu, le résumé de la mission doit refléter fidèlement la substance du rapport et ses principales constatations et recommandations. Il sert d'introduction au rapport et en est à ce titre un élément crucial dans la mesure où il s'agit de la partie la plus lue. Il sert par ailleurs souvent de base au communiqué de presse.

Pour chaque rapport d'audit, la synthèse doit respecter le canevas suivant :

- 1) Avant-propos
- 2) Travaux d'audit
- 3) Résultats de la mission
  - Constatations
  - Recommandations
- 4) Conclusions de la Cour
- 5) Remerciements

## 2. La nature de l'audit

Cette partie doit permettre au lecteur de comprendre ce qu'il peut attendre du rapport. Il s'agit de présenter

- la définition de la mission de contrôle, avec en particulier son origine, les domaines audités, le type et l'étendue de l'audit, et éventuellement les études précédentes et/ou en cours ;
- les objectifs de la mission et les questions d'audit ;
- le déroulement de la mission, c'est-à-dire la description du déroulement de la mission d'audit, depuis la décision d'exécution de l'audit jusqu'à la publication du rapport ;
- les bases de référence de l'audit.

## 3. La description du (des) domaine(s) analysé(s)

Il s'agit d'une description de l'activité ou de l'entité auditee (domaine d'activité, missions, principales caractéristiques, organisation, aspects financiers) et des contextes juridique, politique et économique dans lesquels elle évolue.

## 4. Les résultats détaillés de la mission

Cette partie constitue le corps du rapport puisqu'elle décrit de manière détaillée l'analyse menée par la Cour en relation avec les questions d'audit. Celle-ci doit refléter la situation rencontrée et mener aux constatations et recommandations de la Cour.

Pour chaque axe d'analyse de la Cour, les points suivants sont détaillés :

- **L'analyse** de la Cour : les analyses effectuées par la Cour à partir des données collectées ont pour objet de transformer celles-ci en informations probantes ;
- **Les constatations** de la Cour : les constatations sont exposées de manière à mettre en évidence la source et l'étendue des informations probantes obtenues ainsi que les risques qui découlent des constatations (notamment les conséquences en termes d'économie, d'efficience et d'efficacité de la gestion des deniers publics) ;
- **Les recommandations** de la Cour : les constatations sont suivies le cas échéant des recommandations de la Cour ;
- **Les commentaires de l'audité** : ceux-ci seront inclus dans le rapport en regard des constatations et des recommandations de la Cour (voir paragraphe 3.5).

Les axes d'analyse de la Cour peuvent s'articuler autour des questions d'audit. Si ce n'est pas possible, l'équipe d'audit doit s'assurer que les constatations constituent des éléments de réponse aux questions d'audit.

## 5. Les conclusions

Cette dernière partie comprend les observations générales de l'entité contrôlée, les réponses aux questions d'audit et la conclusion générale de la Cour en lien avec les objectifs de l'audit (ont-ils été atteints ?). Elle inclut également les éventuelles clauses de réserve, ainsi que les remerciements.

Le contenu de ces parties est décrit dans le *Manuel de méthodologie générale de la Cour des comptes*, chapitre 5, paragraphe 5.5.2. Un résumé de la structure du projet de rapport est présenté en Annexe 4 du présent manuel.

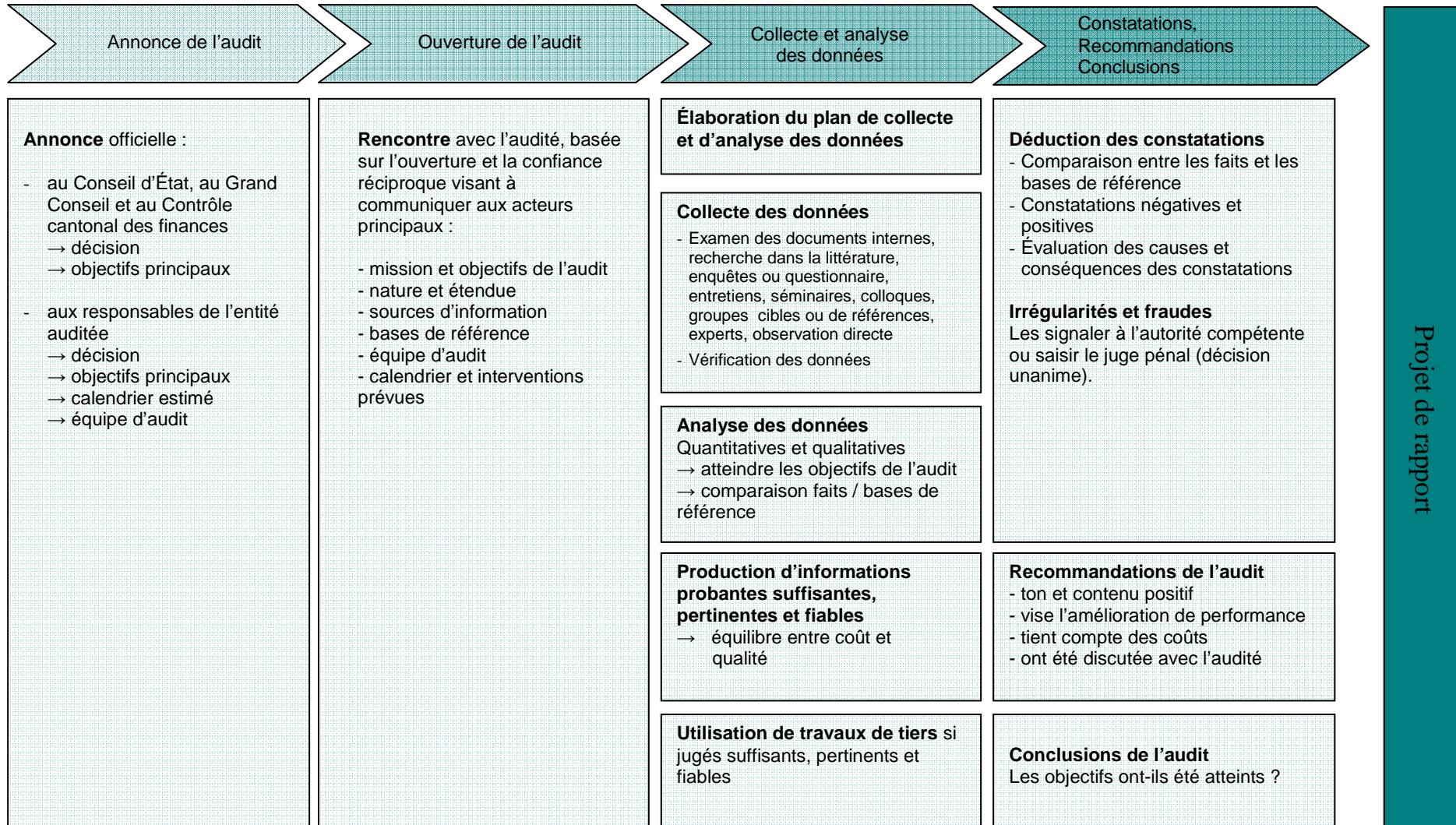
### La validation du projet de rapport

Le projet de rapport est soumis à la Cour, qui décide en séance plénière :

- soit d'approuver le projet de rapport et de démarrer la phase de publication du rapport final selon la procédure décrite au chapitre 3.5.
- soit de récolter des informations complémentaires et/ou de revoir les constatations et/ou les recommandations de l'audit.

La phase d'exécution de l'audit est résumée dans le tableau suivant :

# La phase d'exécution de l'audit



### 3.5. La phase de publication du rapport final

La phase de publication du rapport final commence avec la remise du projet de rapport à l'audité de ses commentaires à la Cour et se termine par la publication ou la décision de ne pas publier le rapport final.

Pour plus de détails, le lecteur se réfère au *Manuel de méthodologie générale de la Cour des comptes*, chapitre 6.

Dès lors que le projet de rapport a été adopté par la Cour, il est transmis à l'audité qui dispose de 21 jours pour prendre position sur les constatations et recommandations. La Cour organise ensuite la séance de clôture de l'audit, au cours de laquelle les points de divergence peuvent être discutés. Les commentaires de l'audité, ainsi que la position finale de la Cour, sont ensuite inclus dans le rapport en regard des constatations et des recommandations. La Cour complète les commentaires de l'audité par sa prise de position finale. Le rapport final est ainsi constitué.

Le rapport final est soumis pour adoption à la Cour en séance plénière. La Cour doit examiner si des intérêts publics ou privés prépondérants s'opposent à la publication du rapport ou de certains de ses éléments (art. 36 LCComptes), puis décider de sa publication ou non.

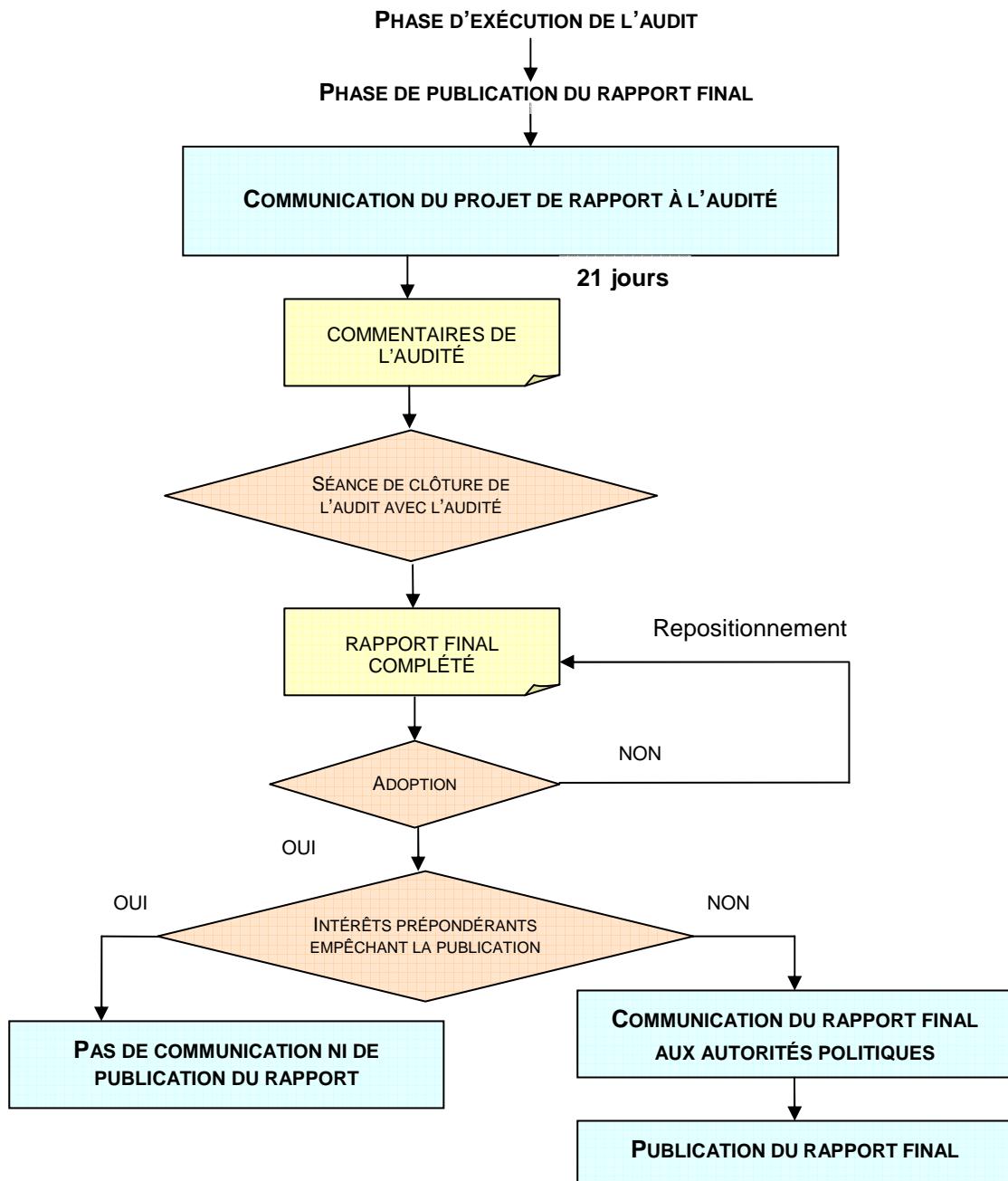
Seule la Cour des comptes étant habilitée à procéder à la publication du rapport, celui-ci doit rester strictement confidentiel jusqu'à sa publication par la Cour. La publication doit ensuite être effectuée dans un délai rapide, de manière à être pleinement utile à ses utilisateurs.

Conformément à l'art. 36 §4 de la Loi sur la Cour des comptes, « *avant de le publier, la Cour des comptes transmet son rapport final à l'entité contrôlée, au Conseil d'État, au Contrôle cantonal des finances, ainsi qu'aux Commissions de gestion et des finances du Grand Conseil* ».

Le rapport est diffusé de la manière suivante :

- par l'envoi du rapport aux parties intéressées autres que l'entité contrôlée et les pouvoirs publics ;
- par la mise à disposition du rapport sur le site internet de la Cour des comptes ;
- par l'envoi aux médias d'un communiqué de presse ;
- par la tenue éventuelle d'une conférence de presse.

La phase d'établissement et de publication du rapport est résumée dans le schéma suivant :



### 3.6. Le suivi du rapport

La loi sur la Cour des comptes ne prévoit pas le suivi par la Cour de la mise en œuvre des recommandations et le retour d'information par l'entité auditee. Elle postule en effet que le suivi relève prioritairement des compétences des destinataires de l'audit.

Néanmoins,

- afin de mettre en place des incitations et au développement des ses membres et de son personnel,
- afin d'améliorer l'efficacité des rapports d'audit,
- afin d'évaluer l'efficacité de la Cour,

la Cour se tient au courant de l'évolution des domaines qu'elle a audités, en se concentrant sur la question de savoir si les points faibles identifiés ont été corrigés, plutôt que de savoir si des recommandations spécifiques ont été mises en œuvre. Dans ce sens, la Cour s'informe auprès de l'entité auditee dans un délai de six mois à une année après la publication du rapport des effets de ses recommandations.

## ANNEXES

Annexe 1	Check-list pour la vérification de l'évaluation de la gestion des risques	p. 58
Annexe 2	Structure du rapport	p. 75

## ANNEXE 1

# CHECK-LIST POUR LA VERIFICATION DE L'EVALUATION DE LA GESTION DES RISQUES

Afin de mener à bien sa mission de vérification, la Cour a intégré les divers éléments du modèle développé au chapitre 2.3 dans une check-list lui servant d'outil de vérification.

La check-list a pour objectif de permettre l'identification des mesures mises en œuvre vis-à-vis des bonnes pratiques en matière de gestion des risques afin d'élaborer des constatations et recommandations.

### Structure et utilisation de la check-list

- La colonne A « Éléments attendus de gestion des risques » présente une liste des éléments requis pour chacune des huit composantes de la gestion des risques selon le modèle exposés sous le chapitre 2.3.
- La colonne B « Éléments de la gestion des risques de l'audité » sert à identifier si, sur la base des entretiens menés et des documents examinés par la Cour, l'élément prévu par le modèle et indiqué dans la première colonne est présent ou non dans le processus de gestion des risques de l'audité.
- La colonne C « Éléments probants » permet d'indiquer, dans le cas où il a été conclu que l'élément mentionné dans la première colonne existe dans la gestion des risques de l'audité (coché oui dans la 2<sup>e</sup> colonne), quels éléments probants ont été rassemblés par l'équipe d'audit afin d'étayer cette conclusion. La check-list comprend certains exemples.
- La colonne D « Évaluation » inclut l'évaluation de la qualité des éléments requis pour les diverses composantes sur la base de l'échelle suivante :
  - 1 = élément inexistant ;
  - 2 = élément existant, de manière complète mais non vérifiable (éléments probants insuffisants) ;
  - 3 = élément existant, de manière incomplète mais vérifiable ;
  - 4 = élément existant, de manière développée et vérifiable ;
  - 5 = élément existant, de manière optimisée (stratégie et performance).Cette évaluation est destinée à guider l'élaboration des constatations, recommandations et conclusions (voir page de conclusion de la check-list).
- La colonne E « Commentaires » permet à d'inclure des explications en relation avec la notation donnée.
- La colonne F « Référence » est utilisée par la Cour pour le classement de la documentation rassemblée.

## Check-list de vérification de l'évaluation de la gestion des risques

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
I. Environnement interne					
1. Les principes de gestion des risques de l'entité sont communiqués a) une politique interne écrite spécifique à la gestion des risques de l'entité existe b) les principes de gestion des risques de l'entité sont évoqués ou rappelés dans d'autres politiques internes c) le personnel est informé par d'autres biais (p. ex : formation) d) la direction est assurée que l'ensemble du personnel est informé	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	- Politique interne - Convocation à une séance de formation - ...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
2. La surveillance qu'exerce la direction est adéquate car elle est a) indépendante b) compétente (expérience suffisante) c) suffisante	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
3. Les valeurs d'éthique de l'entité et les questions d'intégrité et de conflits d'intérêts sont mises en avant a) un document interne existe b) le personnel est informé par d'autres biais (p. ex : formation) c) la direction est assurée que l'ensemble du personnel est informé	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	- Code de conduite - Lignes directrices - ....	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
4. 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.	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Politique interne</li> <li>- Code de conduite</li> <li>- ...</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
5. La structure et l'organisation de l'entité sont <ul style="list-style-type: none"> <li>a) clairement définies et documentées</li> <li>b) adaptées à sa taille et la complexité de ses tâches</li> </ul>	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Organigramme</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
6. La délégation des pouvoirs et responsabilités fait l'objet d'un règlement qui <ul style="list-style-type: none"> <li>a) prend en compte la politique des risques de l'entité</li> <li>b) est connu de l'ensemble des collaborateurs</li> </ul>	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Règlement de signature / de compétences</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
7. Les processus et normes régissant l'attribution des droits d'accès aux systèmes et aux locaux sont définis et connus.	<input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Procédure de gestion des droits d'accès</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
8. La concordance entre le cahier des charges et les compétences du collaborateur engagé pour le poste est assurée et périodiquement vérifiée.	<input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Procédure d'engagement des collaborateurs</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
9. Les mesures relatives au suivi du développement des compétences des collaborateurs sont édictées et disponibles.	<input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Politique de formation</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
10. Il est démontré que les règles relatives à la rémunération et aux promotions ne contiennent pas d'incitations matérielles ou d'objectifs irréalistes susceptibles de générer un comportement immoral ou malhonnête des collaborateurs.	<input type="checkbox"/> oui <input type="checkbox"/> non	<ul style="list-style-type: none"> <li>- Politique de rémunération et de promotion</li> </ul>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		

**Évaluation globale de la composante « Environnement interne »**

- 1 : n'existe pas
- 2 : existe mais n'est pas documenté
- 3 : existe de manière incomplète mais vérifiable
- 4 : existe de manière développée et vérifiable
- 5 : existe de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
II. Définition des objectifs					
11. Les objectifs de l'entité sont définis formellement	<input type="checkbox"/> oui <input type="checkbox"/> non	- Stratégie de l'entité	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
12. Les objectifs définis incluent : a) les objectifs stratégiques b) les objectifs opérationnels c) la qualité des informations financières d) la conformité aux lois et règlements applicables	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	- Stratégie de l'entité	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
13. Les objectifs définis sont communiqués à l'ensemble du personnel	<input type="checkbox"/> oui <input type="checkbox"/> non	- Communication interne - Séance de formation	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

#### Évaluation globale de la composante « Définition des objectifs »

- 1 : n'existe pas  
 2 : existe mais n'est pas documentée  
 3 : existe de manière incomplète mais vérifiable  
 4 : existe de manière développée et vérifiable  
 5 : existe de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
III. Identification des événements					
14. L'identification a été effectuée par les personnes les plus compétentes pour l'effectuer (implication des responsables opérationnels à tous les niveaux et de la direction)	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
15. Une méthode reconnue d'identification a été suivie : a) la comparaison avec un catalogue des risques b) un <i>brainstorming</i> ou groupe de travail c) des entretiens d) un questionnaire ou enquête e) autres	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non	- Catalogue des risques utilisé - Convocations - Procès-verbaux - Questionnaire - ...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
16. Tous les types de facteurs ont été considérés a) économiques b) environnementaux c) politiques d) sociaux e) technologiques f) infrastructures g) personnel h) processus	<input type="checkbox"/> oui <input type="checkbox"/> non <input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
17. L'inventaire est documenté.	<input type="checkbox"/> oui <input type="checkbox"/> non	- Catalogue des risques de l'entité	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		
18. L'inventaire est-il mis à jour régulièrement ?	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> 1 2 3 4 5		

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
19. Les opportunités ont également été prises en considération ?	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

**Évaluation globale de la composante « Identification des événements »**

1 : n'existe pas

2 : existe mais n'est pas documentée

3 : existe de manière incomplète mais vérifiable

4 : existe de manière développée et vérifiable

5 : existe de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
IV. Évaluation des risques					
20. L'évaluation est effectuée par les personnes les plus compétentes pour l'effectuer (implication des responsables opérationnels à tous les niveaux et de la direction).	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
21. La période considérée pour l'évaluation est cohérente avec celle fixée pour la réalisation des objectifs.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
22. La fiabilité des données est vérifiée.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
23. En cas d'événements corrélés, l'évaluation a été effectuée de manière groupée.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
24. L'échelle d'évaluation est définie et communiquée/expliquée aux évaluateurs.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
25. L'évaluation des risques des divers services a été consolidée à la fin du processus.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
26. L'évaluation initiale porte sur les risques inhérents.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
27. Le résultat de l'évaluation des risques est documenté.	<input type="checkbox"/> oui <input type="checkbox"/> non	- Cartographie des risques	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

## Évaluation globale de la composante « Évaluation des risques »

- 1 : n'existe pas
- 2 : existe mais n'est pas documentée
- 3 : existe de manière incomplète mais vérifiable
- 4 : existe de manière développée et vérifiable
- 5 : existe de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
V. Traitement des risques					
28. L'évaluation des solutions est effectuée par les personnes les plus compétentes (implication des responsables opérationnels à tous les niveaux et de la direction)	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
29. Une solution a été adoptée pour chacun des risques évalués	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
30. Une évaluation précise de la meilleure réponse est effectuée systématiquement.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
31. La fiabilité des données est vérifiée.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
32. Les réponses aux risques (et les opportunités) sont documentées.		- Plan d'action	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
33. Les réponses aux risques choisies sont approuvées par les personnes autorisées..	<input type="checkbox"/> oui <input type="checkbox"/> non	- Plan d'action validé	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
34. Les réponses aux risques sont réévaluées régulièrement.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
35. Le risque résiduel est évalué régulièrement.	<input type="checkbox"/> oui <input type="checkbox"/> non	- Cartographie des risques adaptée	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

## Évaluation globale de la composante « Traitement des risques »

- 1 : n'existe pas
- 2 : existe mais n'est pas documenté
- 3 : existe de manière incomplète mais vérifiable
- 4 : existe de manière développée et vérifiable
- 5 : existe de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
VI. Activités de contrôle					
36. Les activités de contrôles définies pour répondre aux risques directement ou pour s'assurer que les solutions prévues sont appliquées sont définies par écrit (système de contrôle interne).	<input type="checkbox"/> oui <input type="checkbox"/> non	- Matrice de risques et contrôles	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
37. Les activités de contrôles définies sont connues de l'ensemble du personnel.	<input type="checkbox"/> oui <input type="checkbox"/> non	- Directive sur le contrôle interne	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
38. Les activités de contrôles sont vérifiables (évidence du contrôle).	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

**Évaluation globale de la composante « Activités de contrôle »**

--

- 1 : n'existent pas
- 2 : existent mais ne sont pas documentées
- 3 : existent de manière incomplète mais vérifiable
- 4 : existent de manière développée et vérifiable
- 5 : existent de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
VII. Information et communication					
39. Il existe un système d'information fiable assurant que les informations nécessaires à l'exécution des solutions soient identifiées, collectées et communiquées dans un format et délai approprié.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
40. Le résultat de l'évaluation des risques (identification, évaluation et solutions) est communiqué à tout le personnel.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
41. Les responsabilités de chaque employé envers les réponses à l'évaluation des risques sont clairement définies et communiquées.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
42. Un canal de communication permet aux employés d'informer leur hiérarchie sur les possibilités d'optimisation, les défauts, erreurs ou abus constatés.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

**Évaluation globale de la composante « Information et communication »**

- 1 : n'existe pas
- 2 : existe mais n'est pas documentée
- 3 : existe de manière incomplète mais vérifiable
- 4 : existe de manière développée et vérifiable
- 5 : existe de manière optimisée (stratégie et performance)

A. Éléments attendus de gestion des risques	B. Éléments de la gestion des risques de l'audité	C. Éléments probants (description)	D. Évaluation	E. Commentaires	F. Références
VIII. Pilotage					
43. Un dispositif continu de pilotage est en place (p. ex : rapports réguliers) afin que la direction soit assurée de la bonne exécution des solutions et informée des défaillances.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
44. Lorsqu'une défaillance apparaît, il est assuré que celle-ci soit traitée dans les meilleurs délais.	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		
45. Des évaluations spécifiques ponctuelles du processus de gestion des risques sont effectuées ?	<input type="checkbox"/> oui <input type="checkbox"/> non		<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5		

**Evaluation globale de la composante « Pilotage »**

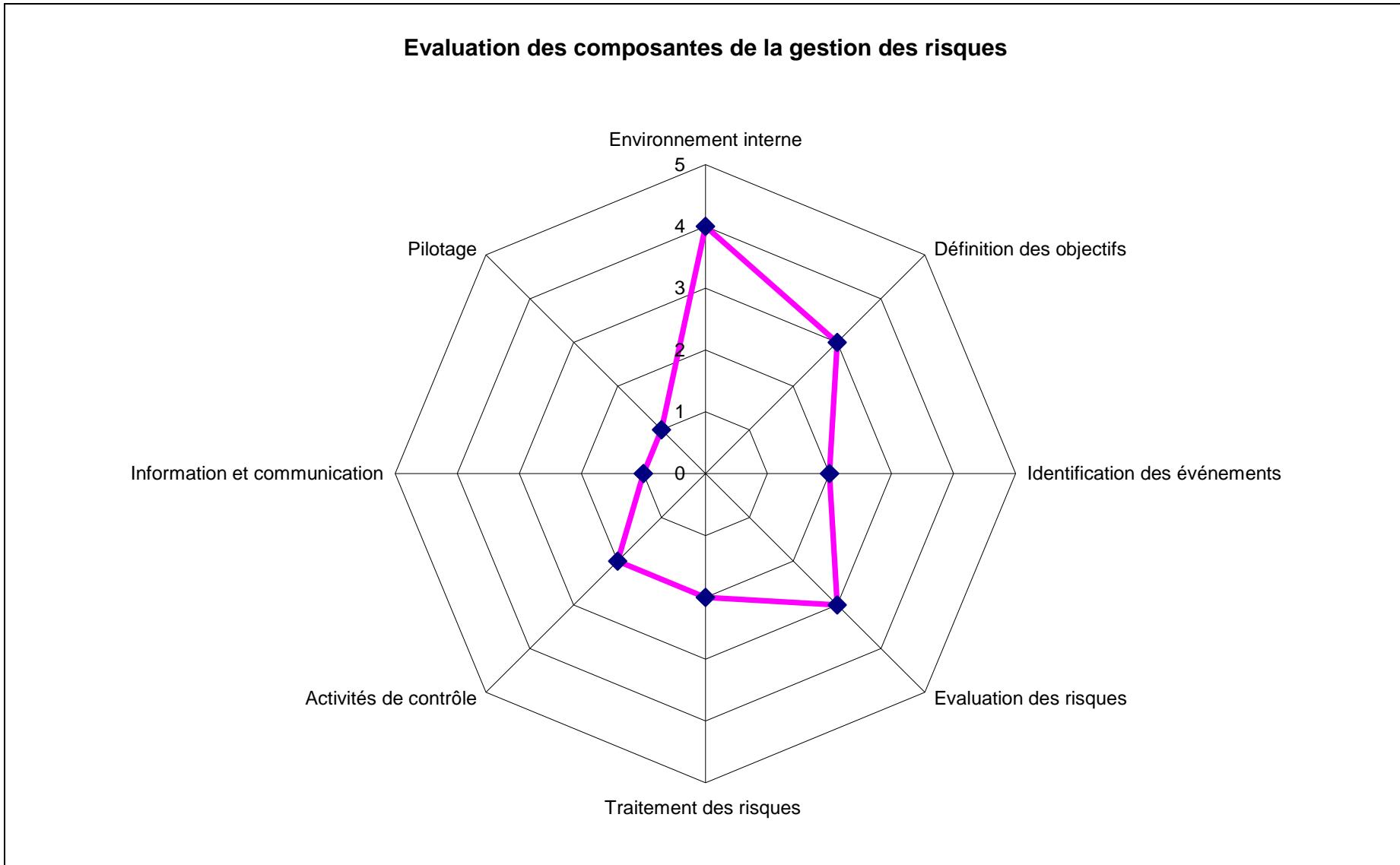
- 1 : n'existe pas  
 2 : existe mais n'est pas documenté  
 3 : existe de manière incomplète mais vérifiable  
 4 : existe de manière développée et vérifiable  
 5 : existe de manière optimisée (stratégie et performance)

## Évaluation finale des composantes de la gestion des risques :

Composantes de la gestion des risques	Évaluation (report)
I. Environnement interne	
II. Définition des objectifs	
III. Identification des événements	
IV. Évaluation des risques	
V. Traitement des risques	
VI. Activités de contrôle	
VII. Information et communication	
VIII. Pilotage	

1 : n'existe pas  
2 : existe mais n'est pas documenté  
3 : existe de manière incomplète mais vérifiable  
4 : existe de manière développée et vérifiable  
5 : existe de manière optimisée (stratégie et performance)

## Représentation graphique de l'évaluation finale des composantes de la gestion des risques



## Évaluation globale de la gestion des risques :

Optimisée	L'ensemble des composantes existent de manière très développée et sont documentées. Elles sont optimisées à travers une réelle politique globale de gestion des risques.	L'entité utilise la gestion des risques comme un <b>outil de pilotage stratégique</b> , ainsi que dans la mesure de performance.
Intégrée	L'ensemble des composantes existent de manière très développée et sont documentées.	La gestion des risques est intégrée aux activités opérationnelles. Le <i>reporting</i> et l'allocation des ressources sont ajustés aux résultats de l'analyse des risques. Des ajustements rapides peuvent être effectués lorsque les conditions évoluent. L'entité utilise la gestion des risques comme un <b>outil de gestion opérationnelle</b> .
Établie	L'ensemble des composantes existent et sont documentées. Toutefois, les composantes « environnement interne », « information et communication » et/ou « pilotage » pourraient être renforcées.	L'entité a mis en place une structure de gestion des risques avec des responsabilités claires. Les principes de la gestion des risques sont décrits de manière détaillée et communiqués au sein de l'entité. L'analyse est menée de manière régulière et quantifie les risques opérationnels de manière anticipée. Elle est suivie d'une stratégie de réduction des risques et est documentée. L'entité utilise la gestion des risques comme un <b>outil d'aide à la décision</b> .
De base	Certaines composantes sont peu développées et/ou peu ou pas documentées. Les composantes « environnement interne » et « information et communication » sont insuffisamment développées.	L'entité dispose d'une gestion des risques centralisée, menée sur une base annuelle, mais limitée et non standardisée et peu documentée. Elle fait l'objet d'un <i>reporting</i> minimal. L'objectif poursuivi est de démontrer que l'entité dispose d'un dispositif minimum de gestion des risques ( <b>conformité</b> ).
Inexistante	La majorité des composantes n'existent pas.	Il n'existe pas de gestion des risques.

La Cour admet que la gestion des risques d'une entité est considérée comme acceptable à partir d'une évaluation « Établie ».

## ANNEXE 2

## STRUCTURE DU RAPPORT

1. **Synthèse**  
Résumé de la mission de contrôle  
Liste des constatations et des recommandations
2. **Nature de l'audit**
  - 2.1. Définition de la mission de contrôle
    - 2.1.1. Origine de la mission
    - 2.1.2. Domaine(s) audité(s)
    - 2.1.3. Type et étendue de l'audit
    - 2.1.4. Etudes précédentes et/ou en cours
  - 2.2. Objectifs de la mission et questions d'audit
  - 2.3. Déroulement de la mission
  - 2.4. Bases de référence
3. **Description du (des) domaine(s) analysé(s)**
  - 3.1. Contextes juridique, politique et économique
  - 3.2. Présentation de l'entité auditée, ses missions et ses principales caractéristiques
4. **Résultats détaillés de la mission de contrôle**
  - 4.1. Axe d'analyse 1
    - 4.1.1. Analyse de la Cour
    - 4.1.2. Constatations
    - 4.1.3. Recommandations
    - 4.1.4. Observations de l'audité
  - 4.2. Axe d'analyse 2
    - 4.2.1. Analyse de la Cour
    - 4.2.2. Constatations
    - 4.2.3. Recommandations
    - 4.2.4. Observations de l'audité
  - 4.3. ...
5. **Conclusions**
  - 5.1. Observations générales de l'entité auditée
  - 5.2. Réponse aux questions d'audit
  - 5.3. Conclusion générale de la Cour (les objectifs ont-ils été atteints ?)
  - 5.4. Remerciements

## BIBLIOGRAPHIE

### Bases légales :

- *Constitution vaudoise* du 14 avril 2003 instituant la Cour des comptes
- *Loi sur la Cour des comptes* du 21 novembre 2006 (LCComptes)
- *Exposé des motifs et projet de loi sur la Cour des comptes* (no 344 - mai 2006)
- *Loi sur les finances* du 20 septembre 2005 (LFin)

### Ouvrages de référence de gestion du risque :

- *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), « *Enterprise Risk Management — Integrated Framework* », 2004
- *Institut de l'Audit Interne*, PricewaterhouseCoopers et Landwell & Associés, « *Le management des risques de l'entreprise — Cadre de référence — Techniques d'application* », Éditions d'Organisation, Groupe Eyrolles, 2005

### Publications spécifiques à la gestion du risque :

- *Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public — Informations complémentaires sur la gestion des risques des entités* (INTOSAI GOV 9130)
- Brochure *Politique de gestion des risques — Bases pour la gestion des risques au sein de la Confédération* de décembre 2004

### Sites internet :

- Cour des comptes européenne : <http://eca.europa.eu>
- Bureau du vérificateur général du Canada : <http://www.oag-bvg.gc.ca>
- Contrôle fédéral des finances : <http://www.efk.admin.ch>

### Autres :

- Article « *Évaluation des risques et systèmes de contrôle interne* » par B. Chapuis et B. Perrin, *L'expert comptable suisse*, numéro 9/2008