

Audit interne et référentiels de risques

VERS LA MAÎTRISE DES RISQUES
ET LA PERFORMANCE DE L'AUDIT



Du même auteur, Pierre Schick

- *Guide d'audit des achats et des ventes*, Eyrolles, 2014.
- *Mémento d'audit interne*, Dunod, 2007.
- *Guide de self-audit*, Éditions d'organisation, 2^e éd., 2002.

Mise en page : [Belle Page](#)

© Dunod, 2021
11, rue Paul Bert, 92240 Malakoff

<http://www.dunod.com>

ISBN : 978-2-10-082304-8

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2^o et 3^o a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Sommaire

[Couverture](#)

[Page de titre](#)

[Page de Copyright](#)

[Avant-propos](#)

[Préface](#)

[Introduction](#)

[Partie 1 - L'environnement de l'audit interne](#)

[Chapitre 1 - Le périmètre d'intervention de l'audit](#)

[Le gouvernement d'entreprise](#)

[Le management des risques](#)

[Le contrôle interne](#)

[Chapitre 2 - La fonction d'audit interne](#)

[L'audit interne et son évolution](#)

[Une profession qui s'appuie sur des normes](#)

[L'Institut français de l'audit et du contrôle internes \(IFACI\)](#)

[Les fonctions voisines de l'audit interne](#)

[Chapitre 3 - L'organisation de l'activité d'audit](#)

[Le rattachement de l'audit interne](#)

[La charte de l'audit interne](#)

[L'organisation des moyens](#)

[La gestion des auditeurs](#)

[La nécessité de se former](#)

[La communication de l'audit interne](#)

[Les mesures de satisfaction et de performance de l'audit](#)

Chapitre 4 - L'identification des besoins d'audit

L'élaboration d'une cartographie des risques

L'établissement du plan et du planning d'audit

Partie 2 - La méthodologie de l'audit

Chapitre 5 - Les processus de conduite d'une mission

Chapitre 6 - Les modalités d'application (MA)

Le droit d'accès : la lettre ou l'ordre de mission

L'examen de l'activité et son découpage en « objets auditables »

Référentiel d'audit : l'élaboration d'un tableau des risques

La réunion d'ouverture ou d'installation de l'équipe

L'analyse des forces et faiblesses

Le rapport d'orientation ou la note de cadrage

Le programme de vérification

La conduite des vérifications et la formalisation des travaux de contrôle

La fiche d'audit et de recommandations (FAR)

L'ossature du rapport

Le compte rendu oral sur site

Le rapport d'audit et sa validation

Le suivi des recommandations

L'état des actions de progrès

Chapitre 7 - Les documents associés (DA)

Ordre de mission

Tableau des risques

Rapport d'orientation

Programme de vérification

Budget – planning

Feuille de couverture de test

Feuille de couverture d'entretien

Fiche d'audit et de recommandations

Projet de rapport d'audit

[Rapport d'audit](#)
[Suivi des recommandations / plan d'actions](#)
[État des actions de progrès](#)
[Fiche de conseils de perfectionnement post-audit](#)
[Questionnaire de satisfaction post-audit](#)

Partie 3 - Les outils de l'audit interne

Chapitre 8 - Les techniques d'audit traditionnelles (TA)

[L'analyse économique et financière](#)
[Les volumes et types de transactions](#)
[Les diagrammes de circulation \(flow charts\)](#)
[La grille de séparation des tâches](#)
[Les interviews](#)
[Les questionnaires administrés](#)
[La piste d'audit](#)
[Les observations physiques](#)
[Les rapprochements et reconstitutions](#)
[L'interrogation des fichiers informatiques](#)
[Les sondages statistiques](#)

Chapitre 9 - Les nouveaux outils liés aux évolutions technologiques

[Une approche contemporaine de l'audit](#)
[Une approche des risques intégrant la gestion des autorisations \(droits, données et SOD\)](#)
[Les pratiques actuelles et évolutions liées au numérique](#)
[L'analyse des données \(data analytics\)](#)
[L'exploration des données \(data mining\)](#)
[L'intelligence artificielle](#)
[Audit interne et intelligence artificielle \(IA\)](#)
[L'apport d'une solution de type hub collaboratif pour piloter un audit interne](#)

Partie 4 - Les référentiels de risques – Illustrations et cas pratiques

Chapitre 10 - Les tableaux des risques

La structuration et le mode d'utilisation des référentiels

Approche globale

Approche par processus ou domaines de gestion

Chapitre 11 - Illustrations et cas pratiques

QUIZ

Illustrations des 17 principes du COSO

Étude de cas : société H.A.

Conclusion générale

Avant-propos

Depuis le début des années 2000, plusieurs réglementations et législations en provenance des États-Unis (Sarbanes Oxley Act), de l'Union européenne (4^e et 7^e directives, Règlement général sur la protection des données, RGPD) ou de France (loi LSF du 1^{er} août 2003, loi du 3 juillet 2008, loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « Sapin 2 ») ont renforcé les exigences en matière de contrôle interne et de gestion des risques. De manière indirecte, le rôle de l'audit interne – chargé d'évaluer les processus de management des risques, de contrôle interne et de gouvernement d'entreprise – s'en est trouvé accru.

Dans cet ouvrage, les auteurs présentent les étapes méthodologiques à respecter pour améliorer l'efficacité de la mission d'audit interne, tout en recherchant la conformité avec le Cadre de référence international des pratiques professionnelles en la matière. Pour chaque étape, des conseils et des fiches pratiques complètent les propos. La méthodologie et les quinze référentiels de risques présentés s'appuient sur le dispositif de contrôle interne et de gestion des risques préconisé par l'AMF et le référentiel COSO de contrôle interne en vigueur depuis 2013.

Cette troisième édition actualise les sections développées dans l'édition de 2014 et enrichit le retour d'expérience méthodologique réalisé auprès de plusieurs directions d'audit interne. Elle développe un chapitre consacré aux nouveaux outils liés aux évolutions technologiques.

Pour approfondir le contenu de cet ouvrage et illustrer nos propos, vous pouvez accéder à des vidéos en ligne sur un site dédié :

<http://www.audit-interne-referentiels-risques.fr/>,

mais aussi réaliser un quiz et un cas pratique, disponibles en fin d'ouvrage.

Le contrôle interne joue un rôle important en ce sens qu'il permet de réduire les risques d'erreurs, mais il contribue aussi à une meilleure maîtrise des processus et permet d'améliorer la capacité d'une organisation à réaliser les objectifs fixés par la direction générale.

La maîtrise et la gestion des risques sont devenues un véritable enjeu. Or, si cet enjeu est essentiel dans le cadre de la conduite des opérations – car celle-ci doit anticiper au mieux les risques dans un environnement plus large et plus mouvant –, il l'est également au titre de la communication financière et extra-financière.

Cet ouvrage insiste sur le fait qu'un dispositif d'audit et de contrôle interne ne doit jamais rester statique, car les organisations sont en perpétuelle évolution et les systèmes doivent en conséquence être constamment adaptés et modifiés.

Par ailleurs, l'audit interne d'une organisation doit se concentrer sur les domaines d'importance majeure afin de répondre aux préoccupations fondamentales des instances dirigeantes.

Dans ce contexte, il est particulièrement utile aux entreprises et à ceux qui, au sein de celles-ci, ont la charge de veiller à la bonne application du dispositif de contrôle interne, de disposer d'outils et d'éléments de réflexion mis à jour des meilleures pratiques, tenant compte des développements conceptuels les plus récents.

Cet ouvrage présente les repères méthodologiques et les fiches opérationnelles nécessaires à la conduite d'une mission d'audit efficace et efficiente.

Les auteurs

Préface

Professionnels, enseignants et étudiants trouveront dans cette nouvelle édition une synthèse de ce qu'il faut savoir pour conduire une action de maîtrise des risques sur les principales activités et processus de l'organisation.

S'appuyant sur le Cadre de référence international des pratiques professionnelles de l'IIA (CRIPP), garant de la qualité des missions d'audit réalisées, il présente une déclinaison de la méthodologie de conduite d'une mission d'audit interne préconisée par l'institut.

Écrit dans un style imagé et illustré de nombreux schémas et tableaux, l'ouvrage présente de façon très concrète et pédagogique les étapes méthodologiques à respecter pour améliorer l'efficacité d'une mission d'audit. Pour chaque étape, des fiches pratiques, des « focus », des retours d'expérience et des documents standards illustrent et complètent les propos.

L'ouvrage souligne l'intérêt de développer des outils innovants de modélisation, d'optimisation et de partage des connaissances permettant de réconcilier la méthode (la théorie), l'expérience (les référentiels de risques) et la doctrine (les référentiels de contrôle interne) en démontrant l'intégrité de l'ensemble.

Les dimensions contrôle interne et management des risques sont traitées en adéquation avec les référentiels COSO – contrôle interne (2013), COSO ERM et le cadre de référence de l'AMF 2010.

Il s'agit d'un livre utile, opérationnel et sa lecture sera particulièrement bénéfique à tous ceux qui souhaitent améliorer leur pratique de l'audit interne.

Philippe MOCQUARD
Délégué général de l'IFACI ¹

[1.](#) Le contenu de cet ouvrage ne peut engager l'IFACI et reste le fruit de ses auteurs.

Introduction

Pour assurer sa pérennité et son développement, toute organisation, qu'elle soit publique ou privée, grande ou petite, doit se fixer des objectifs. Une fois cet horizon stratégique établi, il s'agit de définir les moyens nécessaires pour y parvenir et de veiller à leur bonne mise en œuvre. Enfin, il faut s'assurer que l'organisation a atteint ses objectifs initiaux, afin de « boucler la boucle ». Ce triptyque « Objectifs – Moyens nécessaires – Pilotage/Contrôle » résume très brièvement la démarche stratégique traditionnelle pratiquée, de façon plus ou moins formelle, dans toutes les organisations. Ces préoccupations sont généralement dévolues à la direction générale et aux instances composant la gouvernance (conseil d'administration ou de surveillance, comité de direction, comité d'audit...).

Dans nos environnements économiques actuels instables, l'atteinte de ces objectifs n'est évidemment pas certaine. L'organisation est quotidiennement confrontée à une multitude de risques, d'importance et de nature très différentes, qui peuvent perturber, voire rendre impossible, la réalisation de ses objectifs. Même si l'aversion au risque est dans la nature humaine, en matière de management la prise de risque est vitale pour l'organisation. Un mode de gouvernance qui consisterait à ne s'engager dans telle ou telle orientation stratégique que lorsque toutes les incertitudes sont totalement levées conduirait, du fait d'un manque de réactivité, bien évidemment à la remise en cause à terme de la pérennité de l'organisation concernée.

Donc cette prise de risque est inévitable et nécessaire, cependant elle doit être maîtrisée. Le concept de « contrôle interne », au sens littéral du terme et pris ici dans son acception la plus large (processus de gestion des risques, de contrôle et de gouvernance d'entreprise), correspond à la mise en œuvre de dispositions qui assurent une maîtrise raisonnable des risques d'une organisation afin de lui

permettre d'atteindre ses objectifs. Le contrôle interne est donc un élément fondamental de l'environnement de contrôle de toute structure, quels que soient sa taille, son secteur d'activité, son environnement. Concernant la pérennité et le développement des organisations, l'absence de préoccupation en matière de contrôle interne serait tout aussi préjudiciable qu'une frilosité excessive dans la prise de risques découlant d'une stratégie timorée.

Enfin le contrôle interne, comme tout système organisationnel, est naturellement sujet à défaillance. Les évolutions externes ou internes impactent systématiquement le système de contrôle interne qui doit s'adapter en permanence. Afin de s'assurer que ces dispositifs de contrôle remplissent parfaitement leurs rôles, les directions générales des organisations se dotent d'un « outil » d'évaluation et de surveillance du contrôle interne : il s'agit bien évidemment de l'activité d'audit interne.

Dans ce rôle d'appréciation de l'existence, de la bonne application et de l'efficacité des dispositifs de contrôle interne, l'audit pourrait donc être qualifié comme étant « le contrôle du contrôle (interne) ».

Cet enchaînement d'étapes : OBJECTIFS – RISQUES – CONTRÔLE INTERNE – AUDIT constitue le fondement du processus de contrôle des organisations.

L'ouvrage s'articule autour de cette logique. Bien qu'il soit centré sur le métier de l'audit interne, il présente dans un premier temps les concepts de gouvernement d'entreprise, de management des risques et de contrôle interne car ils constituent des préalables incontournables pour comprendre la raison d'être de l'activité d'audit interne. D'ailleurs, la définition de l'audit interne, qui est présentée par la suite, ne précise-t-elle pas que ces trois dimensions constituent les principaux champs d'intervention de l'activité d'audit interne ? Il paraissait donc naturel et logique pour chacun d'eux :

- d'en donner une définition officielle ou institutionnelle ;
- de présenter les cadres de références et modèles les plus reconnus qui les conceptualisent ;
- de citer les différents acteurs internes et externes qui agissent sur ces trois registres.

L'ouvrage met ensuite plus particulièrement l'accent sur l'activité d'audit interne à travers notamment :

- *sa méthodologie* : encore plus que tous les autres métiers du management des organisations, l'auditeur interne a besoin et doit suivre une méthodologie d'investigation précise et détaillée. La définition de l'audit interne parle d'« approche systématique et méthodique ». Du respect scrupuleux de cette méthodologie dépendent la qualité des missions d'audit réalisées et donc leur légitimité ;
- *ses outils* : une méthode pour savoir comment faire c'est bien, mais sans outils pour aider à sa mise en œuvre, c'est insuffisant – qu'il s'agisse des outils « traditionnels » (analyses, enquêtes, interviews, sondages statistiques, pistes d'audit, *flow charts*...) ou de ceux issus de la « révolution numérique » ;
- *ses référentiels de risques associés* : parmi toutes les aides à la disposition de l'auditeur interne, les référentiels de risques en constituent un élément essentiel. Véritable cadre de référence dans le déroulement d'une mission d'audit, les référentiels de risques (qu'ils soient établis en phase de préparation d'une nouvelle thématique à auditer ou répertoriés dans une bibliothèque de référentiels existants) représentent une garantie quant à l'exhaustivité des différents thèmes à auditer, au degré de détail approprié des investigations à mener ou encore à l'achèvement de la mission dans les délais prévus.

Cette nouvelle édition s'inscrit bien évidemment dans la continuité de la version précédente. Cependant, nous avons souhaité compléter notre réflexion en y intégrant de nouvelles préoccupations.

Les « métiers du contrôle », dans nos économies actuelles, sont en constante évolution. Nous nous devons donc de relater ces évolutions (lois, règlements, normes...).

La précédente version intégrait les avancées normatives, notamment celles concernant le référentiel de contrôle interne de l'AMF et l'actualisation du modèle de contrôle interne mondialement connu, le COSO version 1992 « désignation COSO1 ». Cette version fondatrice, actualisée en 2013, est maintenant identifiée sous l'appellation de « COSO contrôle interne ». Au-delà de la présentation théorique de ces

référentiels, nous avons souhaité l'illustrer, dans la présente version, par un certain nombre d'exemples montrant comment les grandes entreprises communiquent à ce sujet. Ces illustrations sont disponibles sur les sites Internet des entreprises concernées.

La méthodologie d'audit présentée dans cet ouvrage est le résultat de nos connaissances et expériences respectives dans ce domaine. Il nous semblait utile de comparer la méthodologie proposée à celles pratiquées aujourd'hui par divers services d'audit interne. Cette nouvelle version relate donc une synthèse de cette démarche de *benchmark*, réalisée dans un cadre universitaire auprès de grandes entreprises nationales et internationales.

Enfin, nous avons complété cette nouvelle édition d'illustrations de ce que font les entreprises sur ces thématiques, en évoquant l'impact de la « révolution numérique » sur les métiers de l'audit et en proposant des études de cas.

Les auteurs

Partie 1

L'environnement de l'audit interne

[Le périmètre d'intervention de l'audit Chapitre 1](#)

[La fonction d'audit interne Chapitre 2](#)

[L'organisation de l'activité d'audit Chapitre 3](#)

[L'identification des besoins d'audit Chapitre 4](#)

Chapitre 1

Le périmètre d'intervention de l'audit

EXECUTIVE SUMMARY

- Les processus de management des risques, de contrôle et de gouvernement d'entreprise sont les trois principaux périmètres d'intervention de l'auditeur. Vous trouverez dans ce chapitre une présentation de ces trois dimensions avec un accent particulier mis sur le contrôle interne.
- De nombreuses réflexions, d'une grande richesse, menées autour de ces concepts par des experts du monde entier (associations professionnelles, instances régulatrices...), vous seront ensuite présentées. Ces divers travaux, notamment les référentiels de contrôle interne, constituent des aides précieuses lors de la mise en œuvre de ces concepts dans les organisations.

LE GOUVERNEMENT D'ENTREPRISE

Le Cadre de référence international des pratiques professionnelles de l'IIA (*Institute of Internal Auditors* – www.theiia.org), traduit en français par l'IFACI (Institut français de l'audit et du contrôle internes – www.ifaci.com, voir sa présentation au chapitre 2, « Une profession qui s'appuie sur des normes ») donne une définition du gouvernement

d'entreprise (ou gouvernance) : « *Dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.* »

L'OCDE (Organisation de coopération et de développement économiques) précise quant à elle : « *Le gouvernement d'entreprise fait référence aux relations entre la direction d'une entreprise, son conseil d'administration, ses actionnaires et autres parties prenantes. Il détermine également la structure par laquelle sont définis les objectifs d'une entreprise, ainsi que les moyens de les atteindre et d'assurer une surveillance des résultats obtenus.* »

L'European Corporate Governance Institute (www.ecgi.org) récapitule les codes en matière de gouvernement d'entreprise de différents pays du monde.

La lecture de ces textes atteste d'une large diversité dans la conception du gouvernement d'entreprise. Cependant, plusieurs principes de base apparaissent souvent et peuvent constituer un socle commun de connaissance des bonnes pratiques de gouvernance. L'IIA en a établi, dans son livre blanc, une liste dont nous présentons ici les principaux éléments :

- s'appuyer sur une organisation qui garantit un bon fonctionnement du conseil (nombre de membres adéquat, existence d'autres comités émanant du conseil, procédures concernant l'organisation des réunions...);
- prévoir que les membres du conseil possèdent les qualifications et l'expérience appropriées ainsi qu'une bonne connaissance du fonctionnement de l'organisation ;
- mettre à disposition du conseil les ressources nécessaires pour des demandes de renseignements complémentaires afin d'en garantir l'indépendance ;
- contribuer à la définition de la stratégie de l'organisation, notamment en dotant les acteurs de la gouvernance des informations nécessaires pour ce faire ;
- contribuer à la définition de la structure organisationnelle qui participe à la réalisation de la stratégie de l'organisation ;

- instaurer une politique de gouvernement d'entreprise concernant la surveillance des résultats obtenus ;
- prévoir les interactions nécessaires entre le conseil, la direction et les auditeurs internes et externes (*via* un comité d'audit) ;
- contribuer à la mise en œuvre d'un système de contrôle interne efficace supervisé par la direction ;
- définir les politiques et pratiques de rémunération, notamment celles concernant la direction générale, en accord avec les valeurs éthiques, les objectifs, la stratégie et l'environnement de contrôle de l'organisation ;
- communiquer, dans l'ensemble de l'organisation, une culture de la déontologie, les valeurs de l'organisation et la nécessité de l'exemplarité de la direction ;
- faire appel de manière efficace aux auditeurs internes qui doivent disposer par ailleurs d'une indépendance pour garantir leur objectivité et de ressources suffisantes pour mener à bien leur mission ;
- faire appel de manière efficace aux auditeurs externes en s'assurant de l'adéquation de leur indépendance, de leurs ressources et de leur champ d'activité ;
- définir et mettre en œuvre des politiques, processus et responsabilités en matière de management des risques au niveau du conseil et dans l'ensemble de l'organisation ;
- communiquer de manière appropriée les informations pertinentes aux parties prenantes ;
- comparer les processus de gouvernement d'entreprise de l'organisation avec les bonnes pratiques reconnues et les réglementations en vigueur.

Tous ces principes concourent à une bonne gouvernance. Comme nous le verrons ultérieurement lors de la présentation de l'audit interne ([chapitre 2, « L'audit interne et son évolution »](#)), la gouvernance constitue un des trois domaines d'intervention de l'auditeur interne, probablement moins fréquemment couvert que ne le sont les deux autres : le management des risques et le système de contrôle interne. Cependant, dans le cas d'une mission d'audit interne qui concernerait

spécifiquement cette dimension, la liste des principes énumérés précédemment pourrait constituer un premier guide d'investigation, l'auditeur interne s'assurant de l'existence, de la diffusion et de l'efficience de tous ces principes et bonnes pratiques.

Au sein du gouvernement d'entreprise, le comité d'audit tient une place prépondérante. La transposition en droit français (article 14 de l'ordonnance du 8 décembre 2008 et articles L 823-19 et L 823-20 du Code de commerce) de la 8^e directive européenne du 17 mars 2006 (obligation pour toute société faisant appel public à l'épargne de disposer d'un comité d'audit) a permis une clarification au niveau du positionnement, du rôle et de la composition des comités d'audit en France, ainsi que de la compétence de leurs membres. Par la suite, un groupe de travail, sous l'égide de l'AMF, a publié à l'été 2010 un « Rapport sur le comité d'audit » qui précise les modalités de fonctionnement de ce comité (périmètre d'intervention, composition, démarche de mise en œuvre...). Il est disponible sur le site www.amf-france.org.

LE MANAGEMENT DES RISQUES

Le concept de risque

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

L'IIA et l'IFACI, dans le glossaire des normes, définissent le risque comme suit : « *La possibilité que se produise un événement susceptible d'avoir un impact sur la réalisation des objectifs.* »

Prenons un exemple dans notre quotidien : la notion de risque est associée d'une part à celle d'incertitude et d'événement incertain – « il risque de pleuvoir » – et d'autre part à ce que l'on encourt si l'événement se réalise – « je risque de me faire tremper ». Dans notre exemple, l'objectif est implicite – « rester sec et net » –, mais il aurait mieux valu l'explicitier.

« Événement incertain qui *a une conséquence dommageable quant à l'atteinte d'un objectif* », est-on exhaustif dans l'appréciation des différents paramètres liés au concept de risque ? Non. Car on ne se fait pas tremper parce qu'il a plu mais à la fois parce qu'il a plu et que l'on n'avait pas de parapluie. L'absence de parapluie devient l'une des causes, et à y réfléchir c'est la cause maîtrisable, donc la cause intéressante.

« Je me suis fait tremper parce que je n'avais pas de parapluie. »

La cause est l'absence de parapluie, la pluie n'est que la circonstance.

Nous donnerons donc la définition suivante du concept de risque :
« *Le risque est un concept signifiant la possibilité que la combinaison d'un événement incertain et d'un mode de fonctionnement aléatoire ait pour conséquence la non-atteinte d'un objectif.* »

Évident ?

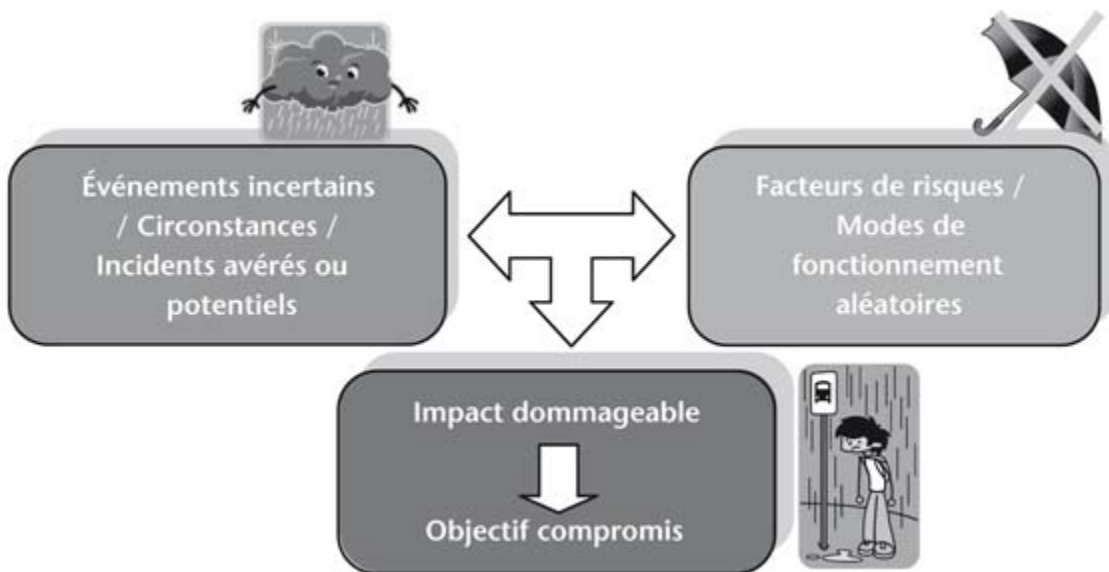
Non, puisque l'on trouve dans la presse des déclarations du genre : telle entreprise est tombée en faillite parce que ses clients ne la payaient pas, ou telle autre a perdu des parts de marché sur sa nouvelle activité pourtant extrêmement innovante au profit d'un concurrent très agressif. Est-ce la faute des clients si la première entreprise est tombée en faillite, ou d'une part à son système de suivi des factures et de relance des impayés et d'autre part à son système de gestion des clients qui la laissait continuer à vendre à des mauvais payeurs ? Et la seconde n'aurait-elle pas dû protéger son innovation par des brevets avant de lancer cette activité qui a nécessité des budgets importants en matière de recherche et développement ?

La pluie, le client mauvais payeur, le concurrent agressif « copieur de nouvelles idées », le comptable qui inscrit un montant erroné ou l'impute à un compte erroné ne sont pas des facteurs de risque : ce sont des événements (et même des événements banals) que l'entreprise doit pouvoir détecter, voire anticiper, pour y faire face.

Figure 1.1 – Le concept de risque



Figure 1.2 – Du concept de risque à sa définition



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

Prenons un exemple : nous redoutons que la salle informatique prenne feu, puis l'ensemble du bâtiment. Pour pallier les risques, nous allons prendre des mesures qui constituent des éléments du dispositif de contrôle interne à mettre en place :

- prévention pour éviter l'incendie : panneaux d'interdiction de manipuler des matières inflammables à proximité de la salle, sensibilisation/formation du personnel concerné au risque d'incendie ;
- détection pour s'apercevoir que l'incident redouté est survenu malgré les mesures de prévention : détecteurs de fumées et de chaleur ;
- protection pour limiter les dégâts occasionnés par l'incendie : *sprinklers* et diffuseurs de gaz inertes, portes coupe-feu... À noter que s'assurer est une mesure de protection : cela limite le coût des dégâts à la franchise.

Cette typologie, qui provient des assureurs, donne de l'imagination à l'auditeur, tant dans sa recherche des facteurs de risques que dans celle des solutions à proposer : un seul type de mesure est rarement efficace, il faut souvent les combiner. Il faut même parfois lutter contre le réflexe naturel : la salle informatique est trop près des cuves à mazout et en dessous du niveau de ruissellement des eaux, l'accident n'est pas encore survenu mais la situation est trop exposée, il faut déménager la salle (prévention). Il est bien plus économique d'accepter les risques d'incendie et d'inondation et d'organiser un système de *back-up* régulièrement testé (protection) !

La figure 1.3 résume donc les différents éléments conceptualisant la notion de risque.

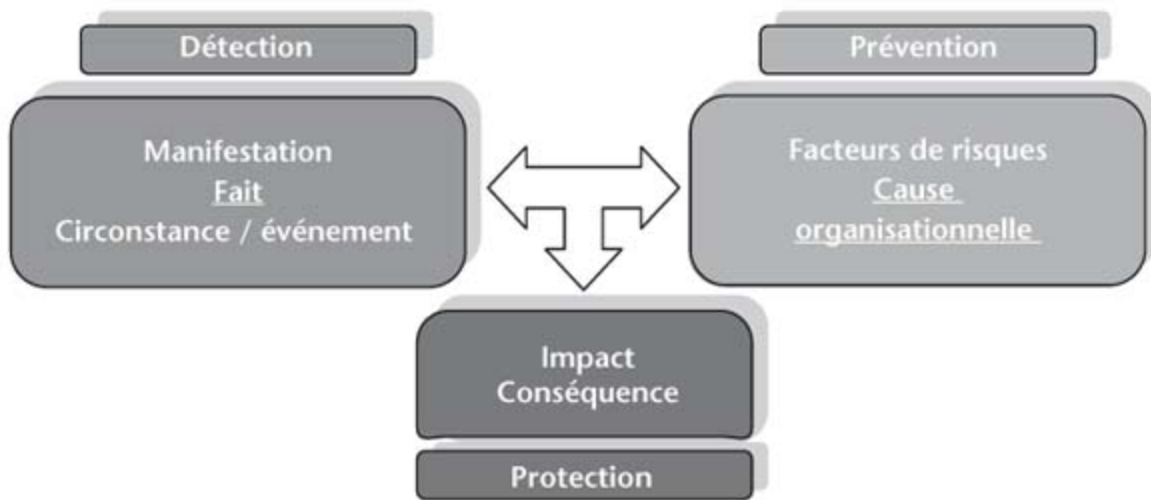
Combinant avec ce qui précède, nous aurons l'équation :

Événement (ou circonstance) + **Cause** (ou facteur de risques) = **Conséquence**

et trois types de mesures pour pallier les facteurs de risques :

Prévention – Détection – Protection.

Figure 1.3 – Le risque et ses composantes



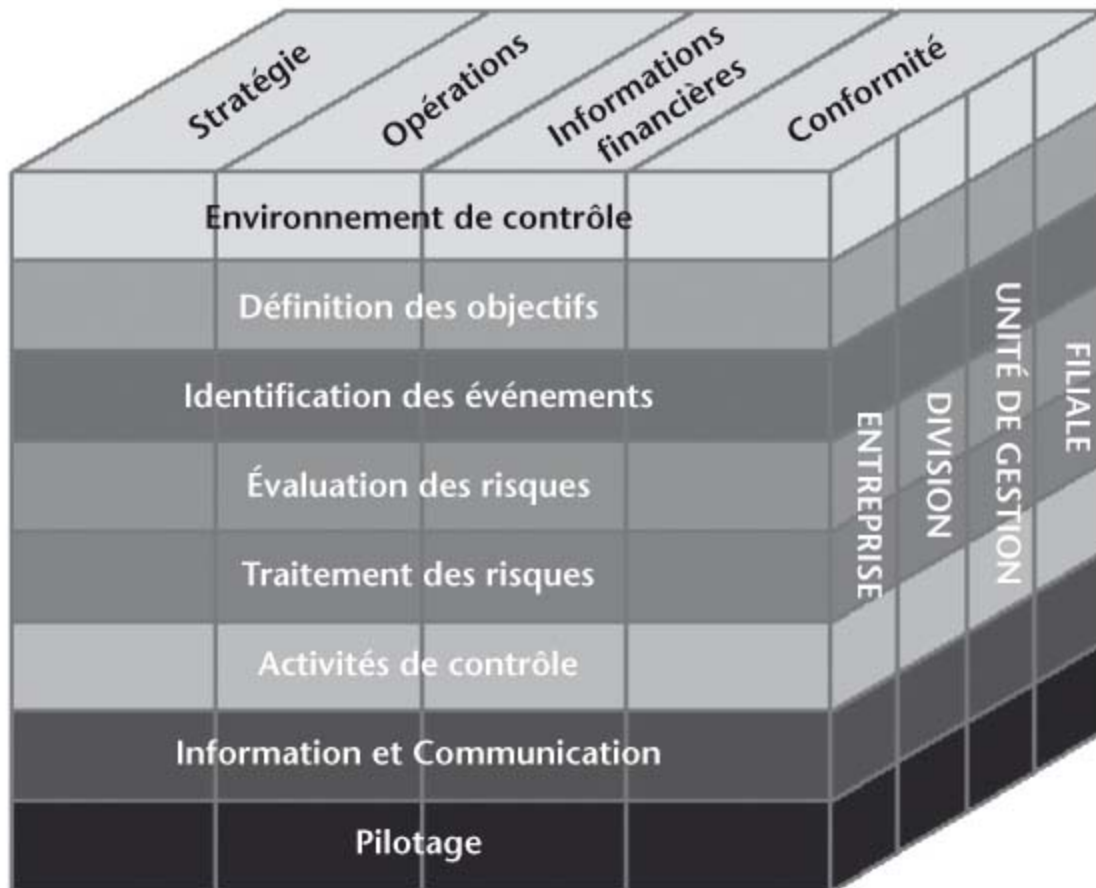
En matière de management des risques, le modèle COSO « ERM » (*Committee Of Sponsoring Organizations of the Treadway Commission, « Enterprise Risk Management »*), constitue une référence internationale pour sa mise en œuvre. Ce cadre de référence donne du management des risques d’une organisation, la définition qui suit : « *Un processus, mis en œuvre par le conseil d’administration, la direction générale, le management et l’ensemble des collaborateurs, pris en compte dans l’élaboration de la stratégie de l’organisation ainsi que dans toutes les activités et conçu pour identifier les événements potentiels pouvant affecter l’organisation et gérer les risques dans les limites de son appétence pour le risque afin de donner une assurance raisonnable quant à la réalisation des objectifs de l’organisation.* »

Ce modèle est traditionnellement représenté par un cube.

Face supérieure du cube, les objectifs de l’organisation :

- *objectifs stratégiques* : objectifs de niveau le plus élevé, liés à la stratégie de l’organisation ;
- *objectifs opérationnels* : objectifs généraux concernant l’utilisation efficace et efficiente des ressources ;
- *objectifs de reporting* : objectifs axés sur la fiabilité des informations financières (externes et internes) ;
- *objectifs de conformité* : objectifs visant à la conformité aux lois et règlements en vigueur.

Figure 1.4 – Le cube du COSO « ERM »



Face avant du cube, les composantes du management des risques :

- *un environnement interne de contrôle* qui constitue le fondement structurel du système de management des risques et qui intègre des aspects très divers tels que la culture du risque et l'appétence pour le risque, l'intégrité et les valeurs éthiques, l'engagement de compétence, la structure organisationnelle, les délégations de pouvoirs, de responsabilités, la politique de ressources humaines, la fixation des objectifs ;
- *une identification des événements* susceptibles d'affecter l'atteinte des objectifs de l'organisation. Il s'agit aussi bien d'événements pouvant avoir un impact négatif que d'événements pouvant avoir un impact positif, c'est-à-dire des opportunités à saisir que le management doit intégrer dans sa stratégie. Ces événements

peuvent être de différentes natures : économiques, environnementaux, politiques, sociaux, technologiques ;

- *une évaluation des risques*, c'est-à-dire une appréciation quantitative de la probabilité d'occurrence et de l'impact de ces événements ;
- *un traitement des risques*, c'est-à-dire la décision qui doit être prise suite à l'évaluation des risques. Parmi les alternatives possibles, on choisira entre l'évitement (supprimer le risque en cessant l'activité à l'origine du risque), la réduction (mettre en œuvre des dispositions pour réduire la probabilité et/ou l'impact du risque), le partage (recours à l'assurance, à des opérations de couvertures ou à l'externalisation de l'activité concernée) ou enfin l'acceptation (compte tenu du coût des dispositions à mettre en œuvre, l'organisation préfère accepter le risque en l'état) ;
- *des activités de contrôle* : il s'agit des politiques et procédures mises en place qui permettent de s'assurer que les risques sont bien maîtrisés. Ces dispositions regroupent des modalités telles que les revues du management, la supervision directe d'une activité ou d'une fonction, la séparation des tâches, les contrôles intégrés dans le traitement de l'information, les contrôles physiques, les indicateurs de performance ;
- *l'information et la communication* : les informations pertinentes sont identifiées, saisies et communiquées dans un format et dans des délais permettant à chacun de s'acquitter de ses responsabilités ;
- *le pilotage* : il s'agit aussi bien des activités quotidiennes de contrôle par le management que des démarches d'auto-évaluation ou encore de l'intervention des auditeurs internes ou externes.

Enfin, la face latérale du cube (Filiale, Unité de gestion, Division, Entreprise) symbolise le caractère multidimensionnel du management des risques et la nécessité de l'adapter à l'entité concernée. De nombreux paramètres peuvent impacter le management des risques tels que la taille de l'organisation, sa culture du contrôle, son secteur d'activité, les réglementations en vigueur.

On notera que le référentiel COSO « ERM » a évolué en 2017 et souligne l'importance de prendre en considération les risques tant dans

le processus d'élaboration de la stratégie que dans le pilotage de la performance. En résumé, le conseil du COSO indique que cette mise à jour :

- éclaire l'intérêt du management des risques de l'entreprise lors de l'élaboration et de la mise en œuvre d'une stratégie ;
- renforce l'articulation entre la performance et le management des risques de l'entreprise afin d'améliorer la définition des objectifs de performance et la compréhension de l'impact des risques sur la performance ;
- tient compte des attentes en matière de gouvernance et de surveillance ;
- reconnaît la mondialisation des marchés et des activités ainsi que la nécessité d'avoir une approche à la fois commune et modulée selon les zones géographiques ;
- présente de nouvelles manières d'appréhender les risques liés à la définition et à la réalisation des objectifs dans un contexte de complexité accrue ;
- élargit le reporting pour répondre aux attentes d'une plus grande transparence de la part des parties prenantes ;
- tient compte de l'évolution des technologies et du foisonnement des données et des analyses requises pour étayer la prise de décisions ;
- propose des définitions, des composantes et des principes pour chaque niveau du management impliqué dans la conception, la mise en œuvre et le pilotage des pratiques de management des risques de l'entreprise.

Le modèle COSO « ERM » ne constitue pas la seule référence en matière de management des risques. Des alternatives existent : l'Association européenne des *risk managers* ou FERMA (*Federation of European Risk Management Associations*) propose son modèle. De la même manière, l'ISO (*International Standard Organization*) propose un modèle dans le cadre des normes ISO 31000:2018 sur le management des risques. En 2010, un groupe de travail, sous l'égide de l'AMF, a proposé un cadre de référence concernant « les dispositifs de gestion des risques et de contrôle interne ». Ce document, disponible sur le site de l'AMF, actualise le cadre de référence de

contrôle interne publié en janvier 2007 (que nous présenterons au chapitre suivant) et développe une approche de la gestion des risques dans une vision commune des deux dimensions.

Mais qu'en est-il de la prise en charge de cette dimension management des risques dans les organisations ?

De nombreux acteurs, principalement internes, interviennent dans ce processus. Parmi les principaux, on citera :

- *le conseil d'administration et ses émanations* (comité des risques, comité d'audit...) qui exercent une surveillance (examen du portefeuille de risques au regard de l'appétence de l'organisation pour ceux-ci, contrôle de la qualité du processus de management des risques pour les risques connus) ;
- *le management* : au niveau de la direction générale en tant qu'ultime responsable de l'efficacité du management des risques. Au niveau des différentes directions en tant que responsable de la mise en œuvre des dispositifs concernés sur le terrain ;
- *la direction des risques (fonction risk management) et du contrôle interne* qui assure, à divers titres, une coordination centralisée du management des risques ;
- *la direction financière*, plus particulièrement sur le volet « reporting des informations financières » et *la direction de la compliance* sur la « conformité aux lois et règlements » ;
- *les auditeurs internes* dont le rôle est d'apprécier l'efficacité du processus de management des risques ;
- *les auditeurs externes* dans le cadre de leur mission légale, notamment au niveau de la fiabilité des informations financières.

Concernant la répartition des rôles en matière de prise en charge du management des risques, nous nous devons également de souligner les travaux menés conjointement par la FERMA et l'ECIIA (*European Confederation of Institutes of Internal Auditing*). Cette réflexion a donné lieu à la publication de recommandations : *Monitoring the effectiveness of internal control, internal audit and risk management systems*. L'idée maîtresse de cette étude repose sur le concept des « trois lignes de défense » en matière de maîtrise des risques : les managers et opérationnels responsables des processus, les fonctions support et l'audit interne.

Tableau 1.1 – Les 3 lignes de défense

		Conseil d'administration/Comité d'audit		AUDIT EXTERNE	Régulateurs
Direction générale			3 ^e ligne de maîtrise		
1 ^{re} ligne de maîtrise		2 ^e ligne de maîtrise			
Autres contrôles pilotés par le management	Dispositif de contrôle interne	Contrôle financier Contrôle interne Hygiène, santé, sécurité Systèmes d'information Ressources humaines Services juridiques Contrôle de gestion Gestion des risques Qualité Conformité, compliance ...	AUDIT INTERNE		

LE CONTRÔLE INTERNE

Il est usuel de dire que le contrôle interne est un procédé mis en œuvre par les dirigeants et le personnel d'une organisation, à quelque niveau que ce soit, destiné à leur donner en permanence une assurance raisonnable que :

- les opérations sont réalisées, sécurisées, optimisées et permettent ainsi à l'organisation d'atteindre ses objectifs de base, de performance, de rentabilité et de protection du patrimoine ;
- les informations financières et opérationnelles sont fiables, et les lois, réglementations et directives de l'organisation sont respectées.

Le contrôle interne est un état à atteindre et à maintenir ; c'est un moyen et non un but. La mise en place du contrôle interne fait partie intégrante des attributions de tout responsable. Dans cette mission, l'organisation peut se doter par ailleurs d'un service *ad hoc* chargé de définir et de coordonner la mise en œuvre des dispositifs composant le système et d'en assurer la maintenance. Dans ces conditions, on veillera à ce que l'existence d'un tel service ne conduise pas à la

désappropriation ou au désintérêt du concept de contrôle par les responsables fonctionnels ou opérationnels.

En toutes circonstances, tout responsable doit se poser la question suivante : Dans quelle mesure mon organisation, mes méthodes de travail, mes dispositifs de mesure et de contrôle, mon implication personnelle me donnent-ils une assurance raisonnable quant à :

- *la pertinence de mes objectifs* : cohérence avec les finalités de l'organisation ?
- *l'adéquation « des moyens aux objectifs »* : efficience de l'organisation, adaptation des structures, coordinations des tâches ?
- *la bonne mise en œuvre des moyens* : efficacité du pilotage, existence d'objectifs, animation et suivi ?
- *la qualité et la fiabilité des informations* pour prendre de bonnes décisions ?
- *le respect des principes, politiques, lois, règlements* d'origine interne et externe ?
- *la protection et la sauvegarde du patrimoine* humain, financier, matériel, immatériel (image, savoir-faire, informations...) ?

Pour la mise en œuvre d'un bon contrôle interne, nous disposons d'un certain nombre de modèles conceptuels ou référentiels. Parmi les plus connus et usités, nous en citerons deux :

- le COSO de contrôle interne version 2013 (*Committee Of Sponsoring Organizations of the Treadway Commission* ou *Internal Control Integrated Framework*), d'origine anglo-saxonne ;
- au niveau français, sous l'égide de l'Autorité des marchés financiers, un référentiel de contrôle interne nommé « cadre de référence AMF » a été publié début 2007. Une mise à jour à l'été 2010 a contribué à donner une plus grande homogénéité aux concepts sous-tendant les travaux du comité d'audit, la rédaction du « rapport du président » sur le contrôle interne et la gestion des risques.

Le COSO de contrôle interne version 2013

Ce modèle donne la définition suivante du contrôle interne : « *Le contrôle interne est un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :*

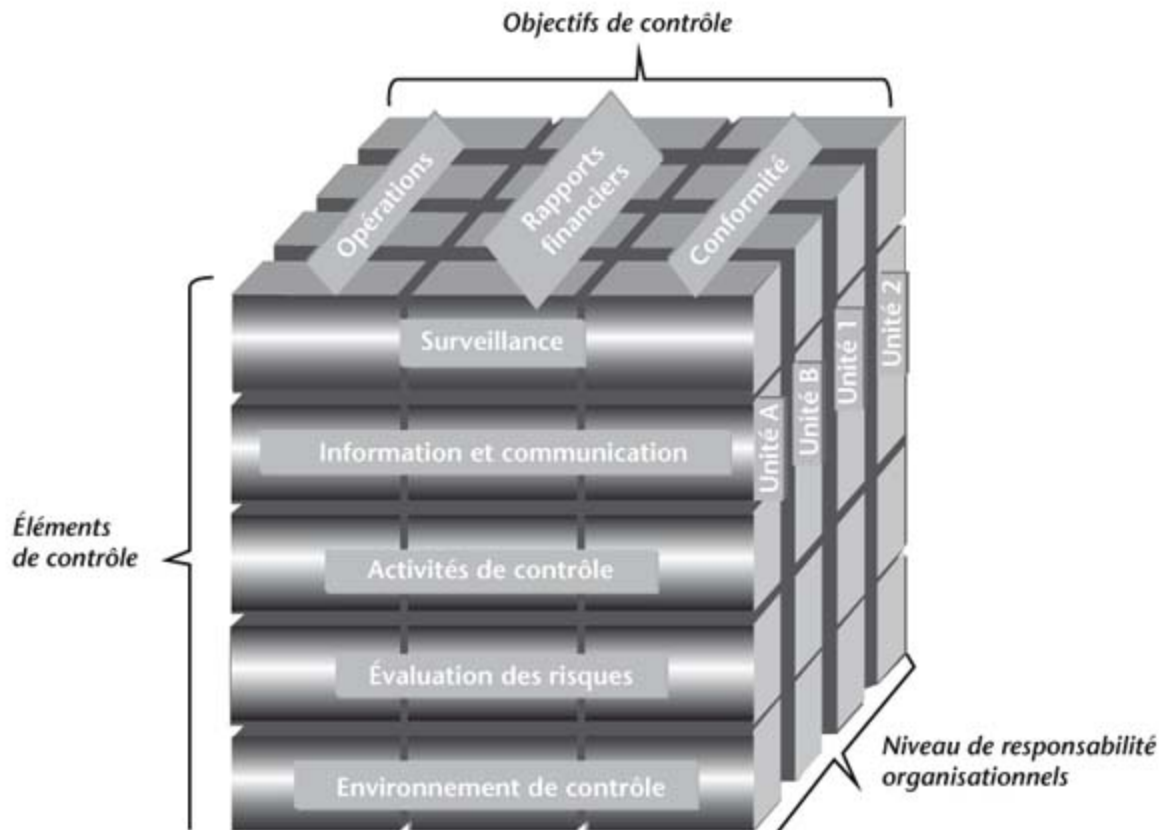
- *réalisation et optimisation des opérations ;*
- *fiabilité des informations ;*
- *respect des réglementations. »*

Le contrôle interne a été schématisé sous la forme d'une pyramide à cinq composantes dans sa version de 1992, puis d'un cube en 2013 :

- environnement de contrôle ;
- évaluation des risques ;
- activités de contrôle ;
- information et communication ;
- pilotage.

Chacune de ces composantes se déclinant ensuite en un certain nombre d'items dont nous donnons quelques exemples dans la figure 1.5.

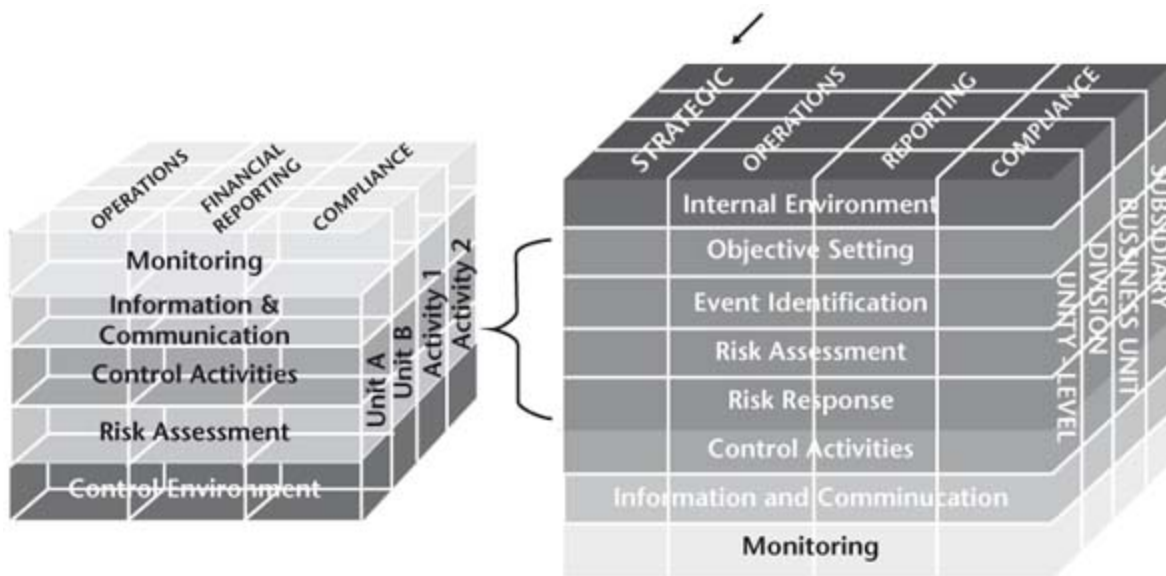
Figure 1.5 – Le cube du COSO de contrôle interne version 2013



Bien que le modèle COSO version 2013 concerne le contrôle interne et le COSO « ERM » le management des risques, les deux cadres de références sont complémentaires (voir [figure 1.6](#)) :

- la composante « Évaluation des risques » du COSO de contrôle interne est déclinée dans le COSO « ERM » en quatre items qui précisent cette notion (la définition des objectifs, l'identification des événements, l'évaluation des risques, le traitement des risques) – *face avant du cube* ;
- une dimension « Stratégie » complète les trois objectifs traditionnels du contrôle interne énoncés dans la définition – *face supérieure du cube*.

Figure 1.6 – Articulation entre le COSO de contrôle interne version 2013 et le COSO « ERM »



Les fondamentaux du référentiel COSO de contrôle interne version 2013 n'ont pas changé. La définition du contrôle interne, les trois objectifs poursuivis et les cinq composantes dans lesquelles se répartissent les dispositifs de contrôle à mettre en œuvre sont conservés par rapport à sa version initiale. Au niveau de sa structuration, la principale nouveauté réside dans les dix-sept principes et les points d'attention associés. La version initiale laissait aux responsables chargés de la mise en œuvre du contrôle interne l'initiative de décliner la nature des différents dispositifs à créer au sein de chacune des cinq grandes composantes du contrôle interne. Sans pour autant constituer un cadre rigide, la nouvelle version apporte à ce niveau une aide indiscutable en guidant l'expert du contrôle interne dans sa mise en œuvre. Les cinq composantes de la version initiale du COSO sont ainsi officiellement déclinées en dix-sept principes complétés par des points d'attention et des illustrations. Le tableau 1.2 précise ces principes de base.

Tableau 1.2 – Les 17 principes du COSO de contrôle interne version 2013

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

Focus

Vous trouverez au chapitre 11 des exemples et illustrations, pour chacun de ces dix-sept principes, montrant comment les grandes entreprises nationales ou internationales communiquent à ce sujet sur leur site Internet.

Le « référentiel AMF »

Ce modèle, publié début 2007, est issu d'un travail réalisé par un groupe de place réunissant les principales instances compétentes en matière de contrôle des organisations, dont l'IFACI. Il est en accord avec la LSF (loi de sécurité financière), compatible avec le COSO et en phase avec les 4^e, 7^e et 8^e directives européennes. Un groupe de travail de l'AMF a revu et amendé en 2010 le cadre de référence de contrôle interne après un examen des référentiels COSO et « Turnbull guidance » britannique en tenant compte des évolutions législatives et réglementaires intervenues en 2008.

Ce cadre donne la définition suivante du contrôle interne : « *Le contrôle interne est un dispositif de la société, défini et mis en œuvre sous sa responsabilité. Il comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques propres de chaque société qui :*

- *contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources, et*
- *doit lui permettre de prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité.*

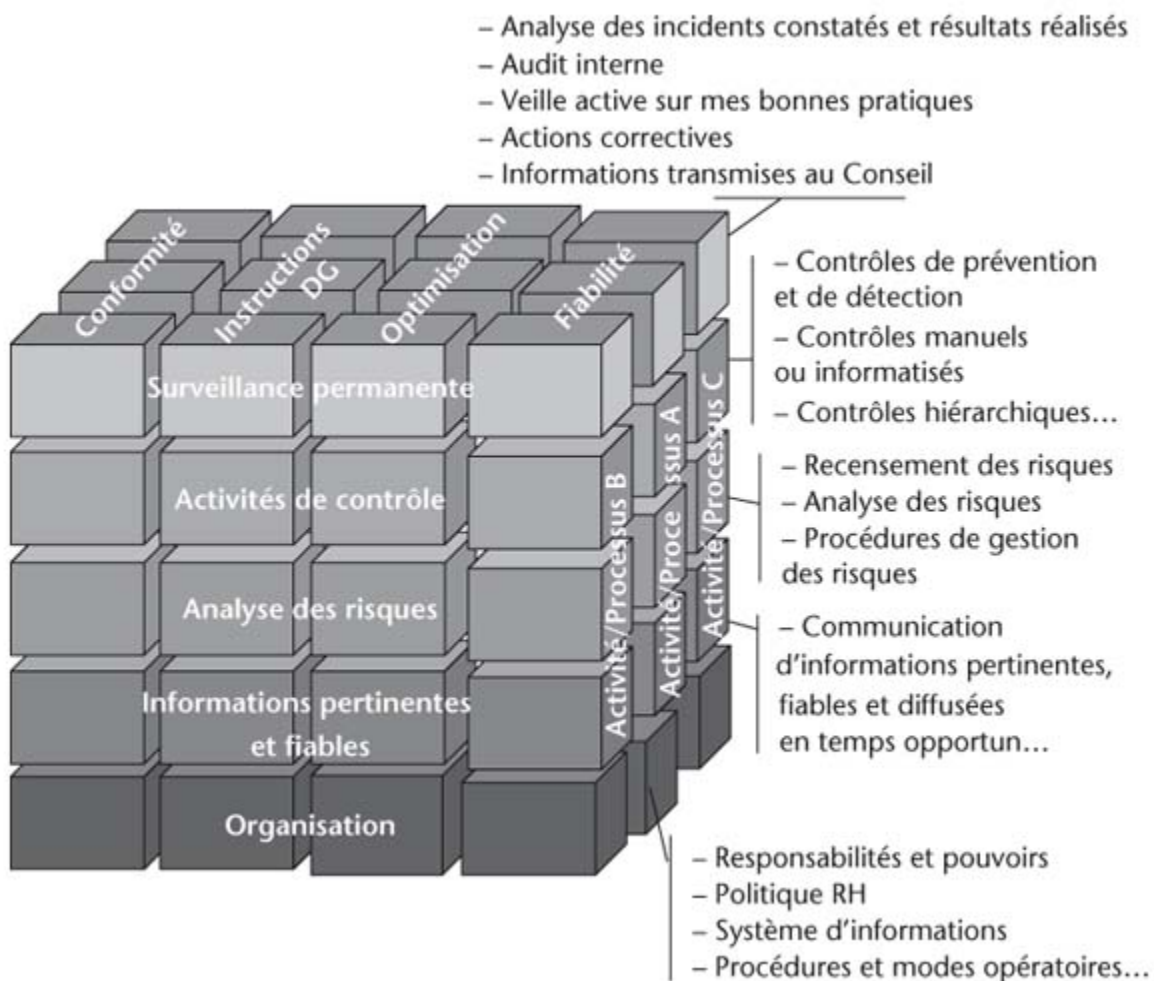
Le dispositif vise plus particulièrement à assurer :

- *la conformité aux lois et règlements,*
- *l'application des instructions et des orientations fixées par la direction générale ou le directoire,*
- *le bon fonctionnement des processus internes de la société, notamment ceux concourant à la sauvegarde des actifs,*
- *la fiabilité des informations financières.*

Le contrôle interne ne se limite donc pas à un ensemble de procédures ni aux seuls processus comptables et financiers. »

Les grandes orientations en matière de contrôle interne sont déterminées en fonction des objectifs de la société. Le contrôle interne est d'autant plus pertinent qu'il est fondé sur des règles de conduite et d'intégrité portées par les organes de gouvernance et communiquées à tous les collaborateurs. L'exemplarité est un principe fondateur, vecteur essentiel de la diffusion des valeurs au sein de la société.

Figure 1.7 – Le « référentiel AMF »



Là aussi, le contrôle interne est défini à travers cinq composantes de base, elles-mêmes se déclinant ensuite en items détaillés :

- une organisation comportant une définition claire des responsabilités, disposant des ressources et des compétences adéquates et s'appuyant sur des systèmes d'information, sur des procédures ou modes opératoires, des outils et des pratiques appropriées ;
- la diffusion en interne d'informations pertinentes, fiables, dont la connaissance permet à chacun d'exercer ses responsabilités ;
- un système visant à recenser, analyser les principaux risques identifiables au regard des objectifs de la société et à s'assurer de l'existence de procédures de gestion de ces risques ;
- des activités de contrôle proportionnées aux enjeux propres à chaque processus, et conçues pour s'assurer que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs ;
- une surveillance permanente portant sur le dispositif de contrôle interne ainsi qu'un examen régulier de son fonctionnement. Cette surveillance, qui peut utilement s'appuyer sur la fonction d'audit interne de la société lorsqu'elle existe, peut conduire à l'adaptation du dispositif de contrôle interne. La direction générale ou le directoire apprécient les conditions dans lesquelles ils informent le conseil des principaux résultats des surveillances et examens ainsi exercés.

Focus

Résultats d'une enquête réalisée par le cabinet KPMG

À la question : « **Quels sont selon vous les risques les plus importants ?** », il a été répondu : Cybersécurité (99 %), Nouvelles technologies (95 %), Environnement réglementaire (92 %), Impact de la digitalisation (88 %), Ubérisation (74 %).

À la question : « **Au regard de ceux-ci, quelles sont les attentes de la gouvernance vis-à-vis des travaux de l'audit interne ?** », il a été répondu : Intégrer les risques émergents dans les plans d'audit (87 %), Faire preuve d'agilité dans l'élaboration des plans d'audit (74 %), Contrôler le fonctionnement des dispositifs de gestion des risques (68 %), Jouer un rôle d'alerte (65 %), Jouer un rôle d'information (19 %).

À la question : « **D'une manière plus globale, quelles sont les attentes de la gouvernance vis-à-vis des fonctions gestion des risques, contrôle et audit internes** »

? », il a été répondu : Identifier et faire remonter les risques émergents (83 %), Fournir une assurance sur la sécurisation des processus (71 %), Apporter du confort sur le fonctionnement du dispositif (69 %), Être acteur dans la création de valeur de l'entreprise (60 %).

À la question : « **Quelles sont les compétences clés à renforcer au sein des équipes audit et contrôle internes ?** », il a été répondu : *Data analytics* (73 %), Systèmes d'informations (71 %), Culture de l'innovation (52 %), Cybersécurité (42 %), *Robotic Process Automation* (42 %), Éthique Conformité (38 %).

À la question : « **Quelles sont les nouvelles technologies qui pourront aider l'audit interne ?** », il a été répondu : Analyse des données pour aider dans l'identification des risques (81 %), Analyse des données pour améliorer les travaux sur le terrain (75 %), Intelligence artificielle (45 %), *Robotic Process Automation* (25 %).

Source : www.kpmg.com, novembre 2018.

N.B. : Le lecteur trouvera par la suite les résultats d'une enquête similaire publiée par l'IFACI, « Risk in Focus 2020 », dont les résultats sont très proches.

L'Essentiel

- La gouvernance (conseil, direction générale...) et ses différentes déclinaisons (comités des risques, d'audit et des comptes, des rémunérations...) définissent les objectifs stratégiques de l'organisation et les moyens nécessaires pour les atteindre, veillent au bon déploiement de ces moyens et enfin s'assurent que les résultats obtenus sont conformes aux objectifs initiaux.
- Le management des risques identifie, classe, hiérarchise les événements potentiels (plutôt d'origine externe) qui, combinés à des facteurs de risques (défaillances plutôt d'origine interne), peuvent entraver l'atteinte des objectifs de l'organisation. Il a également en charge la définition des réponses à apporter aux situations à risques identifiées.
- La mise en place de dispositifs de contrôle interne adaptés est, parmi les réponses possibles à une situation à risques, la solution la plus fréquemment retenue. Le contrôle interne permet de maîtriser, de façon raisonnable, les risques de non-atteinte des objectifs de l'organisation.

Chapitre 2

La fonction d'audit interne

EXECUTIVE SUMMARY

- L'audit interne est une profession qui a une histoire longue. Vous trouverez dans ce chapitre ses origines, ses formes actuelles et ses évolutions.
- Les instances professionnelles (IIA, Institute of Internal Auditors), relayées par l'IFACI (Institut français de l'audit et du contrôle internes), ont souhaité normaliser la profession. À travers ces normes, vous comprendrez ce qu'est l'audit interne mais aussi ce qu'il n'est pas.
- L'audit interne est une fonction de « contrôle », mais elle n'est pas la seule. À la fin de ce chapitre, vous trouverez des comparatifs entre l'activité d'audit interne et les autres fonctions de contrôle.

L'AUDIT INTERNE ET SON ÉVOLUTION

Le temps est révolu où le déclenchement d'un audit interne était reçu par les audités comme un signe de suspicion à leur égard ! Aujourd'hui, le regard de l'audit interne, regard particulier mais professionnel, est apprécié comme un examen salutaire, l'équivalent de la maintenance préventive sur les outils industriels ou de l'assistance dans le diagnostic d'une défaillance repérée. Profession

créatrice de valeur ajoutée, l'audit est un partenaire de la direction générale et du management afin d'accroître et préserver la valeur de l'organisation en donnant avec objectivité une assurance, des conseils et des points de vue fondés sur une approche par les risques.

Le Cadre de référence international des pratiques professionnelles (édition 2017) donne la définition suivante de l'audit interne : *« L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. »*

Cette définition française date du 21 mars 2000. Celle de l'IIA du 29 juin 1999. Les mots clés de la définition de l'audit interne à connaître sont :

- activité ;
- indépendante et objective/impartiale ;
- valeur ajoutée ;
- assurance et conseils ;
- aide à l'atteinte des objectifs ;
- approche systématique et méthodique ;
- évaluation et amélioration ;
- processus de management des risques, de contrôle et de gouvernement d'entreprise.

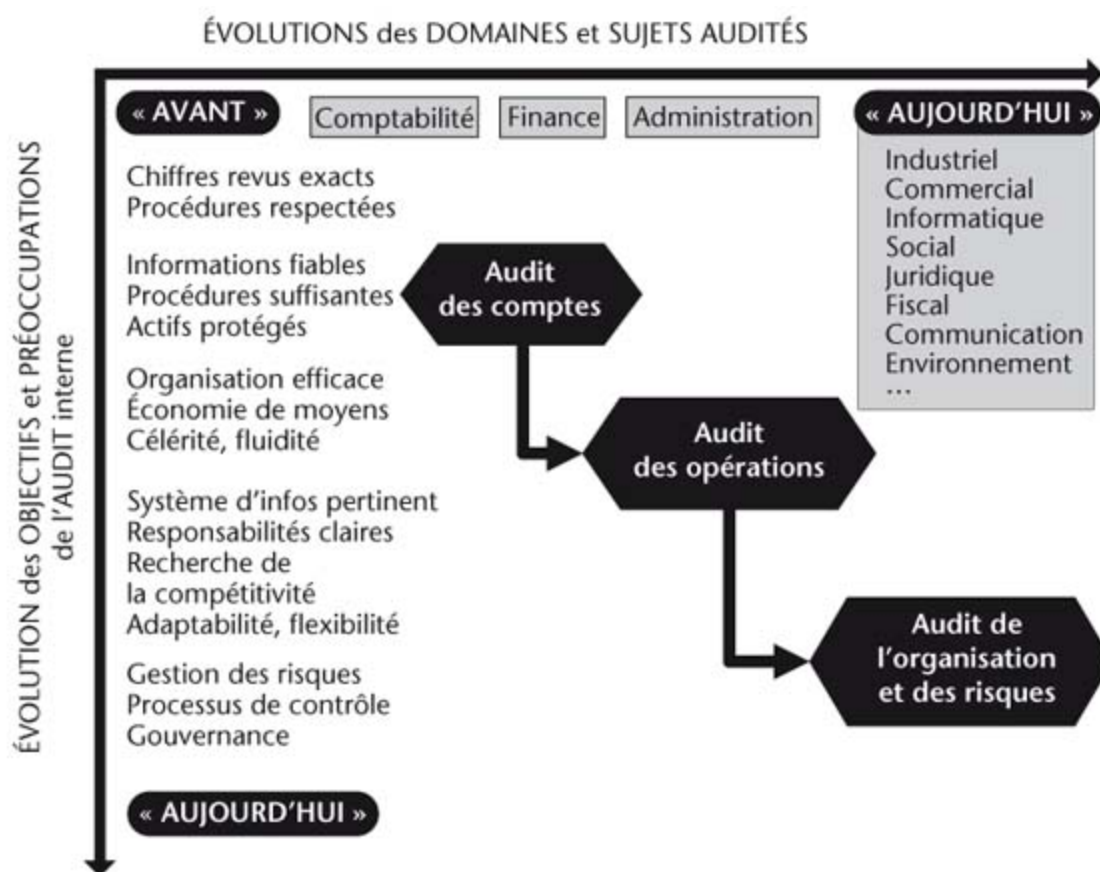
Il est à noter que la définition ne comporte pas les mots « procédures, règles », ni « contrôler, vérifier ». Dans la définition, le mot « contrôle » n'est pas ce que l'audit fait mais ce qu'il évalue et améliore.

L'audit interne décèle les problèmes et formule des recommandations aux directions et aux audités qui leur apportent une solution. Son rôle n'est pas de dénoncer ou d'accuser, mais d'arbitrer les règles du jeu de l'entreprise et surtout de faire pratiquer les « 3R » : Rechercher, Reconnaître et Remédier aux faiblesses de l'organisation.

Il l'aide à anticiper les problèmes et se place dans une démarche vertueuse d'amélioration continue.

Issue du contrôle comptable et financier, la fonction audit interne recouvre de nos jours une conception beaucoup plus large et plus riche, répondant aux exigences croissantes de la gestion de plus en plus complexe des organisations. L'audit interne apporte sa contribution à l'ensemble des activités, fonctions ou processus de l'organisation. Il intervient historiquement dans tous les domaines financiers : comptabilité générale, comptabilité analytique et informations de gestion, trésorerie, crédit/comptabilité/recouvrement clients, aide aux acquisitions et cessions. Celui-ci intervient de nos jours dans tous les domaines de l'organisation. Toutes les entités, activités, fonctions et tous les processus sont concernés par les investigations de l'audit interne. On notera la montée en puissance ces dernières années des audits RSE et liés aux nouvelles réglementations : RGPD, Sapin 2...

Figure 2.1 – L'évolution de l'audit interne



Comme indiqué dans sa définition officielle, l'activité d'audit interne est créatrice de valeur ajoutée et ses principales missions sont d'apporter aux directions générales et comités d'audit un éclairage sur les risques et les systèmes de contrôle interne mais également d'être au service de l'ensemble de l'organisation afin d'apporter une réelle contribution à la gouvernance d'entreprise.

Le processus de management des risques a évolué. L'audit interne est considéré comme un outil de management qui permet de mettre en place une démarche structurée au sein de l'organisation et de travailler en étroite collaboration avec la gouvernance d'entreprise. Le développement des comités d'audit au sein des grands groupes en est le reflet.

Les missions d'assurance prédominent sur celles de conseil :

- *activités d'assurance* : examen objectif d'éléments probants, effectués en vue de fournir à l'organisation une évaluation indépendante des processus de management des risques, de contrôle ou de gouvernement d'entreprise. Par exemple, des audits financiers, opérationnels, de conformité, de sécurité des systèmes et de *due diligence* ;
- *activités de conseil* : conseil et services y afférents rendus au client donneur d'ordre dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectifs de créer de la valeur ajoutée et d'améliorer le fonctionnement de l'organisation. Quelques exemples : consultation, conseil, facilitation, conception de processus et formation.

Pour suivre les évolutions de l'audit interne, on se référera utilement aux enquêtes disponibles sur le site Internet de l'IFACI, ainsi qu'au rapport annuel sur l'état de la profession d'audit interne, publié par le cabinet PWC (www.pwc.com).

L'enquête 2019 s'intitule « Renforcer le rôle de l'audit interne et accroître la digitalisation de la fonction ». Elle révèle que, lorsque les fonctions audit interne s'impliquent dans la transformation digitale (tant pour leur fonction qu'au niveau de l'entreprise), elles aident leurs parties prenantes à gérer les risques de manière plus avisée et à prendre de meilleures décisions.

À la définition officielle de l'audit interne, sont attachés dix principes fondamentaux pour la pratique professionnelle de l'audit interne (voir les dispositions obligatoires dans la base documentaire de l'IFACI) :

- faire preuve d'intégrité ;
- faire preuve de compétence et de conscience professionnelle ;
- être objectif et libre de toute influence indue (indépendant) ;
- être en phase avec la stratégie, les objectifs et les risques de l'organisation ;
- être positionné de manière appropriée et disposer des ressources adéquates ;
- démontrer la qualité de l'audit interne et son amélioration continue ;
- communiquer de manière efficace ;
- fournir une assurance fondée sur une approche par les risques ;
- être perspicace, proactif et orienté vers le futur ;
- encourager le progrès au sein de l'organisation.

Enfin, compte tenu de la confiance placée en l'audit interne pour donner une assurance objective sur les processus de gouvernance, de management des risques et de contrôle, la profession s'est dotée d'un code de déontologie qui va au-delà de la définition de l'audit interne. Ce code de déontologie précise aux auditeurs les valeurs à respecter dans l'accomplissement de leur activité et s'appuie sur quatre principes fondamentaux pertinents pour une pratique « éthique » de l'audit interne.

1. L'intégrité, base de la confiance et de la crédibilité du jugement de l'auditeur.

Les auditeurs internes :

- doivent accomplir leur mission avec honnêteté, diligence, responsabilité ;
- doivent respecter la loi et faire les révélations requises par les lois et les règles de la profession ;
- ne doivent pas sciemment prendre part à des activités illégales ou s'engager dans des actes déshonorants pour la profession d'audit

interne ou leur organisation ;

- doivent respecter et contribuer aux objectifs éthiques et légitimes de leur organisation.

2. L'objectivité, qui permet d'évaluer équitablement tous les éléments pertinents examinés relatifs au domaine audité et de ne pas se laisser influencer dans son jugement. Les auditeurs internes :

- ne doivent pas prendre part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement. Ce principe vaut également pour les activités ou relations d'affaires qui pourraient entrer en conflit avec les intérêts de leur organisation ;
- ne doivent rien accepter qui pourrait compromettre ou risquer de compromettre leur jugement professionnel ;
- doivent révéler tous les faits matériels dont ils ont connaissance et qui, s'ils n'étaient pas révélés, auraient pour conséquence de fausser le rapport sur les activités examinées.

3. La confidentialité concernant les informations reçues et leurs divulgations.

Les auditeurs internes :

- doivent utiliser avec prudence et protéger les informations recueillies dans le cadre de leurs activités ;
- ne doivent pas utiliser ces informations pour en retirer un bénéfice personnel, ou d'une manière qui contreviendrait aux dispositions légales ou porterait préjudice aux objectifs éthiques et légitimes de leur organisation.

4. La compétence requise pour la réalisation des travaux d'audit.

Les auditeurs internes :

- ne doivent s'engager que dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires ;
- doivent réaliser leurs travaux d'audit interne dans le respect des normes internationales pour la pratique professionnelle de l'audit interne ;
- doivent toujours s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.

Focus

L'audit interne est une activité indépendante et objective qui fait partie intégrante de l'organisation. L'audit intervient sur mandat de la direction pour :

- assurer la direction, le conseil et le comité d'audit de l'application des directives et politiques ;
- aider les managers opérationnels et les audités à se contrôler et améliorer leur efficacité.

L'auditeur n'a ni autorité ni responsabilité à l'égard des activités qu'il audite : pas d'affect ni d'intérêt, conditions de l'objectivité.

UNE PROFESSION QUI S'APPUIE SUR DES NORMES

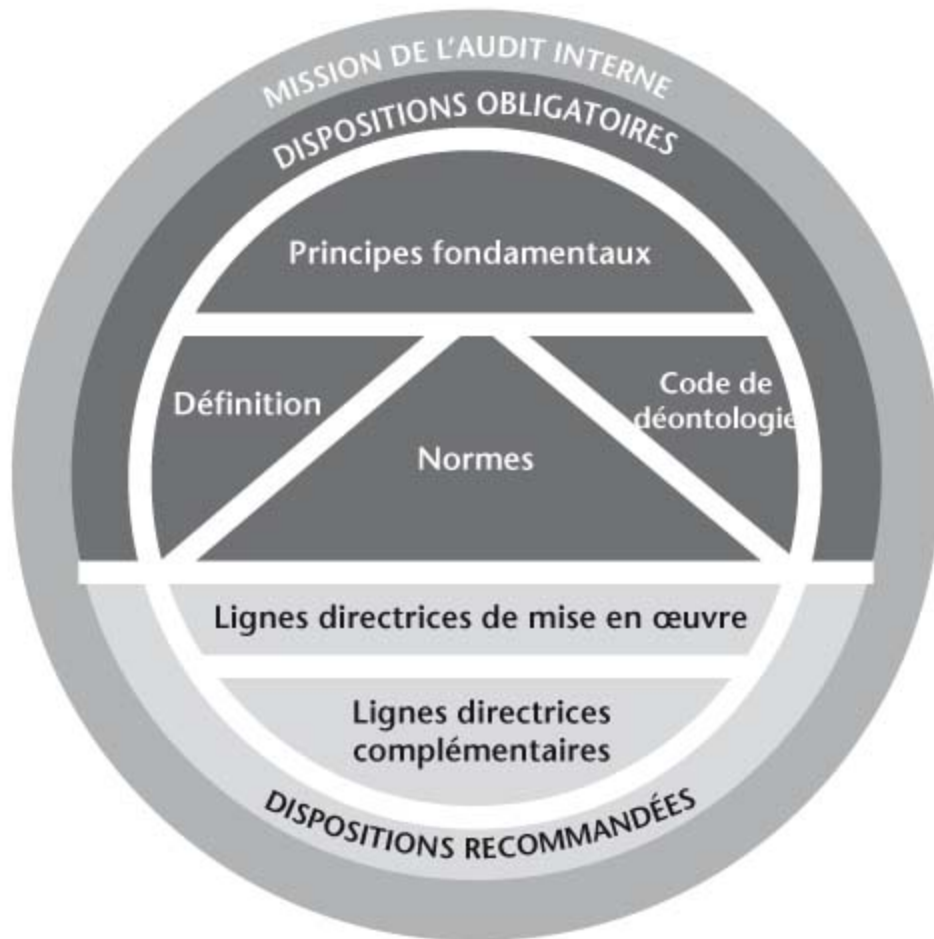
Le métier d'auditeur ne s'improvise pas et s'appuie sur des principes normatifs internationaux. Ces normes sont régulièrement revisitées et la dernière version remonte à l'année 2017.

Les normes de l'audit interne se basent sur le CRIPP (Cadre de référence international des pratiques professionnelles).

Les dispositions obligatoires et recommandées du CRIPP évoluent régulièrement. Elles sont consultables directement sur le site de l'IFACI.

L'audit interne est exercé dans différents environnements juridiques et culturels, au bénéfice d'organisations dont l'objet, la taille, la complexité et la structure sont divers. Il peut être exercé par des professionnels de l'audit, internes ou externes à l'organisation. Comme ces différences peuvent influencer la pratique de l'audit interne dans chaque environnement, il est essentiel de se conformer aux normes internationales pour la pratique professionnelle de l'audit interne.

Figure 2.2 – Les normes de l’audit interne



Focus

Buts explicites : définir les principes de base que la pratique de l’audit interne doit suivre

- Guider l’application des dispositions obligatoires du Cadre de référence international des pratiques professionnelles de l’audit interne.
- Fournir un cadre de référence pour la réalisation et le développement d’un large éventail d’activités d’audit interne à valeur ajoutée.
- Établir les critères d’évaluation et d’appréciation du fonctionnement de l’audit interne.
- Favoriser l’amélioration des processus organisationnels et des opérations de l’organisation.

Buts implicites : un référentiel de réflexion, d’arguments et d’autorité

- Les lire pour réfléchir en s'appuyant sur l'expérience mondiale, se faire une opinion et l'argumenter/la démontrer.
- Les citer en tant que consensus réfléchi de la profession : présomption de pertinence (experts du monde entier) ; autorité dont on peut se prévaloir.

Ces normes aident à répondre aux audités : c'est bien vu et ça les impressionne. Elles suffisent généralement pour ébranler la direction.

Ces normes, qui constituent des exigences minimales, sont subdivisées en :

- « normes de qualification » (séries 1000 à 1322) qui énoncent les caractéristiques des entités et des personnes qui réalisent des activités d'audit interne ;
- « normes de fonctionnement » (séries 2000 à 2600) qui décrivent la nature des activités d'audit interne et définissent des critères de qualité permettant de mesurer leur performance.

Elles sont le plus souvent complétées par des guides de mise en œuvre (GM) qui sont des lignes directrices d'aide à la mise en œuvre permettant aux auditeurs internes d'être en conformité avec les normes.

Chaque guide propose des approches (audit interne, méthodologie et points d'attention). Sur le site de l'IFACI, celles-ci sont au nombre de cinquante-deux, comme les normes.

Focus

Les normes de qualification – séries 1000 à 1322 ***(Ce que sont l'audit interne et les auditeurs)***

- 1000 – Mission, pouvoirs et responsabilités
- 1010 – Reconnaissance des dispositions obligatoires dans la charte d'audit interne
- 1100 – Indépendance et objectivité
- 1110 – Indépendance dans l'organisation
- 1111 – Relation directe avec le Conseil
- 1112 – Rôles du responsable de l'audit interne en dehors de l'audit interne
- 1120 – Objectivité individuelle
- 1130 – Atteinte à l'indépendance ou à l'objectivité
- 1200 – Compétence et conscience professionnelle

1210 – Compétence
1220 – Conscience professionnelle
1230 – Formation professionnelle continue
1300 – Programme d’assurance et d’amélioration qualité
1310 – Exigences du programme d’assurance et d’amélioration qualité
1311 – Évaluations internes
1312 – Évaluations externes
1320 – Communication relative au programme d’assurance et d’amélioration qualité
1321 – Utilisation de la mention « Conforme aux normes internationales pour la pratique professionnelle de l’audit interne »
1322 – Indication de non-conformité

Les normes de fonctionnement – séries 2000 à 2600 *(Ce qu’ils font)*

2000 – Gestion de l’audit interne
2010 – Planification
2020 – Communication et approbation
2030 – Gestion des ressources
2040 – Règles et procédures
2050 – Coordination et utilisation d’autres travaux
2060 – Communication à la direction générale et au Conseil
2070 – Responsabilité de l’organisation en cas de recours à un prestataire externe pour ses activités d’audit interne
2100 – Nature du travail
2110 – Gouvernance
2120 – Management des risques
2130 – Contrôle
2200 – Planification de la mission
2201 – Considérations relatives à la planification
2210 – Objectifs de la mission
2220 – Périmètre d’intervention de la mission
2230 – Ressources affectées à la mission
2240 – Programme de travail de la mission
2300 – Réalisation de la mission
2310 – Identification des informations
2320 – Analyse et évaluation
2330 – Documentation des informations
2340 – Supervision de la mission
2400 – Communication des résultats
2410 – Contenu de la communication
2420 – Qualité de la communication

2421 – Erreurs et omissions
2430 – Utilisation de la mention « Conduite conformément aux normes internationales pour la pratique professionnelle de l’audit interne »
2431 – Indication de non-conformité
2440 – Diffusion des résultats
2450 – Les opinions globales
2500 – Surveillance des actions de progrès
2600 – Communication relative à l’acceptation des risques

L’INSTITUT FRANÇAIS DE L’AUDIT ET DU CONTRÔLE INTERNES (IFACI)

L’IFACI rassemble les professionnels de l’audit et du contrôle internes et, plus largement, de toutes les fonctions contribuant à la maîtrise des risques. L’IFACI est affilié à l’IIA, réseau mondial représentant plus de 200 000 professionnels.

L’IFACI contribue activement à l’évolution des professions de l’audit et du contrôle internes par le partage des meilleures pratiques et la professionnalisation des acteurs et des organisations. Ses adhérents participent au réseau mondial des professionnels de l’audit et du contrôle internes avec des événements, des communautés en ligne et des groupes de travail. Ils trouvent de nombreuses informations sur le site Internet de l’Institut, et notamment des guides et enquêtes qui fournissent des conseils détaillés pour la conduite des activités d’audit interne. On y trouve également des modèles de charte, de gestion de service, des processus (système d’information, contrôle interne, gouvernance, management des risques), des secteurs, des fiches de poste, des guides d’audit, des documents par secteurs (assurance, banque, public) pouvant aider à la mise en place de missions complémentaires (cartographie des risques, audit de PSEE, etc.).

De même, l’IFACI propose une large documentation professionnelle du contrôle interne et du management des risques avec le cadre de référence de ces dispositifs publié en 2010 par l’AMF (Autorité des marchés financiers) ainsi que les principes de mise en œuvre et de

pilotage du référentiel intégré de contrôle interne – COSO – et du management des risques – COSO ERM.

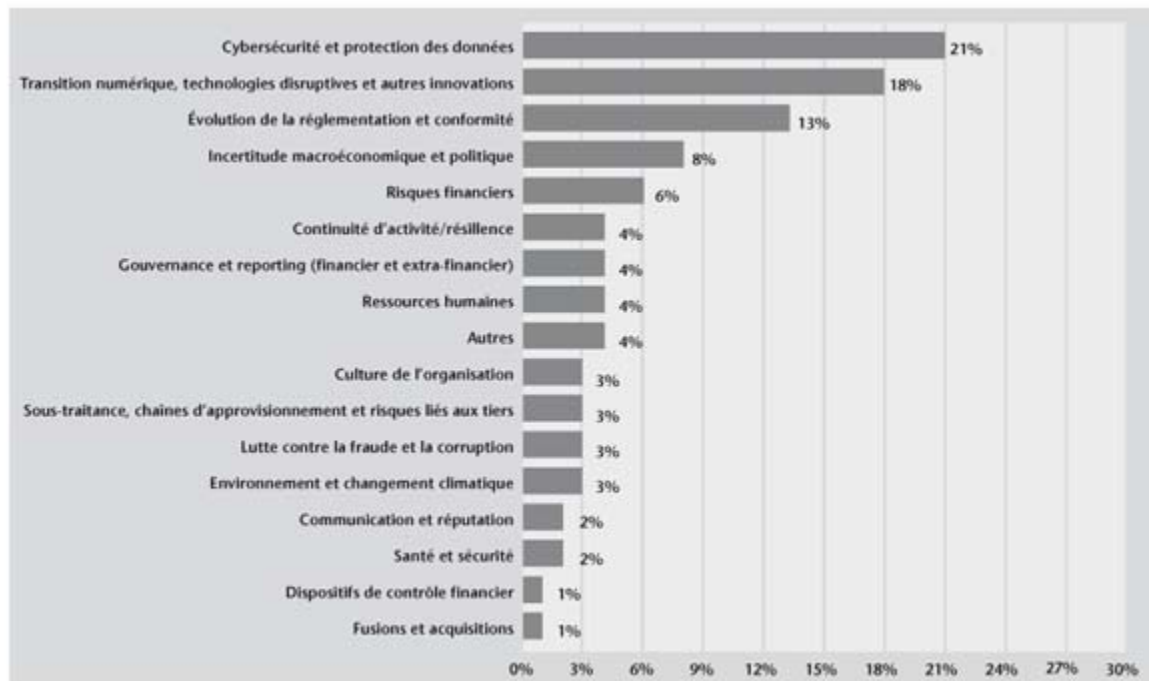
Enfin, les adhérents peuvent accéder à la plateforme Workplace, qui permet aux professionnels de la GRC de se réunir et d'échanger autour de thématiques professionnelles tout en accédant à l'intégralité des services adhérents dont de nombreux magazines, newsletters, enquêtes, en rapport avec les métiers de l'audit interne.

Tous ces documents constituent une véritable manne d'informations que tout professionnel de l'audit se fera un devoir de consulter régulièrement.

En complément au référentiel pour la pratique professionnelle de l'audit interne, chaque année et ce depuis 2017, les huit instituts européens d'audit interne publient une étude intitulée « Risk in Focus » permettant aux directeurs et directrices d'un service d'audit de partager leurs expériences et leurs visions afin de construire une cartographie des risques de l'année à venir.

Pour l'année 2020, les zones de risques prioritaires à adresser sont présentées en figure 2.3.

Figure 2.3 – Cartographie des risques 2020



Source : « Risk in Focus 2020 », IFACI

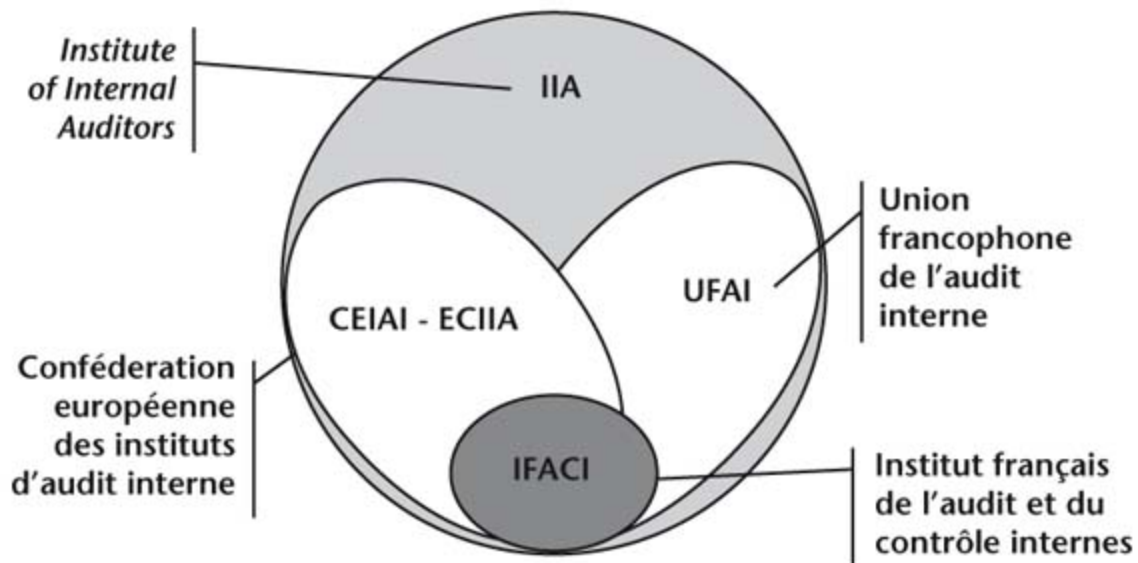
L'IFACI et son réseau proposent un ensemble de certifications reconnues par la profession. Il existe différentes certifications selon votre expérience ou votre spécialité. On retiendra plus particulièrement pour un auditeur :

- la distinction IAP (*Internal Audit Practitioner*) proposée par l'IIA qui atteste des compétences et connaissances fondamentales nécessaires à la pratique de l'audit interne. Elle permet de valoriser son expérience professionnelle en tant qu'auditeur interne et constitue le premier pas vers la certification CIA ;
- le diplôme mondialement reconnu délivré par l'IIA, qui permet d'obtenir le titre d'auditeur interne certifié (CIA®, *Certified Internal Auditor*) et d'être reconnu comme un expert en audit interne quelles que soient sa nationalité et ses formations d'origine ;
- la CPAI (certification professionnelle d'audit interne) que délivre l'IFACI et qui atteste que l'auditeur détient les compétences indispensables à la conduite d'une mission d'audit interne en

conformité avec les meilleures pratiques professionnelles internationales ;

- des certifications professionnelles de l'audit et des systèmes de management, notamment celle délivrée par IFACI Certification qui propose d'une part de certifier le contenu et le niveau de services rendus par la direction d'audit interne par rapport à un référentiel trouvant sa source dans les normes professionnelles et d'autre part de procéder à la certification ISO du système de management de la qualité (démarche d'amélioration continue).

Figure 2.4 – L'audit interne dans le monde. Sa devise : « Le progrès par le partage. »



LES FONCTIONS VOISINES DE L'AUDIT INTERNE

Dans le domaine du contrôle des organisations au sens large, l'activité d'audit interne en est un élément essentiel mais n'en a pas pour autant le monopole. Au fur et à mesure de l'évolution des structures managériales des organisations, diverses fonctions sont

apparues avec chacune leurs spécificités, mais concourant toutes, peu ou prou, aux phases de planification, de mise en œuvre et de contrôle des activités d'une organisation. Nous citerons parmi les missions connexes à l'activité d'audit :

- l'audit externe ;
- le contrôle de gestion ;
- le *risk management* ;
- la conformité (compliance) ;
- la protection des données personnelles ;
- la qualité ;
- la fonction « contrôle interne » ;
- les consultants externes « experts » ;
- les organisateurs internes ;
- l'inspection.

Il nous semble important de situer ces différents interlocuteurs par rapport à l'activité d'audit interne, afin d'une part de préciser les fondamentaux de l'audit interne – ce qui fait sa spécificité – et d'autre part d'apporter une contribution à la clarification d'une situation qui nous semble bien souvent confuse quant aux rôles, pouvoirs et périmètres d'intervention de chacun.

L'audit externe

On assimile souvent l'audit externe au commissariat aux comptes (CAC). Sa mission concerne la certification des états financiers élaborés par l'organisation. Dans la phase intermédiaire de sa mission, dite de contrôles intermédiaires, le CAC est amené à apprécier, comme l'auditeur interne, la qualité du système de contrôle interne. Mais deux aspects distinguent fondamentalement leurs missions respectives. D'une part le CAC se préoccupe de la dimension de contrôle interne principalement et presque exclusivement au niveau du périmètre comptable et financier. Il ne se préoccupe que des processus qui impactent directement les états financiers et n'appréhende pas les autres natures de risques.

D'autre part, lors de ces contrôles intérimaires, l'objectif du CAC est avant tout d'identifier les faiblesses du contrôle interne afin d'orienter ces travaux ultérieurs lors du contrôle final. Il n'a pas, à ce niveau, un véritable rôle de conseil en matière de contrôle interne. Dans sa mission première, il n'a pas à formuler de recommandations quant à son amélioration.

Obligation de résultats ou seulement de moyens ? Le commissariat aux comptes est une profession réglementée et n'a donc juridiquement qu'une obligation de moyens. Mais d'un point de vue commercial il est « préférable » d'apporter des résultats au client.

L'audit interne n'a aucun pouvoir de décision, et certains pensent qu'il ne peut donc avoir d'obligation de résultats, d'autres remarquent que les vendeurs ont des quotas à atteindre alors que ce ne sont pas eux mais les clients qui signent les contrats. L'audit interne n'est pas seul responsable de la réalité du changement, mais il ne peut ignorer sa part de responsabilité, car si les mêmes problèmes réapparaissent, qui peut dire s'il faut l'attribuer à l'insouciance, à l'incompétence des responsables ou au manque de diligence, d'énergie, de persuasion de l'audit interne ? Les documents normatifs internationaux sont clairs : pas d'amélioration, pas de valeur ajoutée !

Tableau 2.1 – Comparaison avec l'audit externe

	AUDIT INTERNE	AUDIT EXTERNE (CAC)
Mandat	De la direction générale, pour les responsables de l'entreprise	Du conseil d'administration (officiellement de l'assemblée générale), pour les tiers qui requièrent des comptes certifiés
Missions	Liées aux préoccupations de la direction générale : découlant de la cartographie des risques. Tous les types d'audit et tous les sujets	Liées à la certification des comptes : mise en œuvre annuelle Audit de régularité uniquement, dans le domaine comptable et financier
Conclusions	Constatations approfondies dès qu'existe un potentiel de dysfonctionnements, pour identifier les causes et définir les actions qu'il y a lieu de mener Obligation de résultats ?	Constatations succinctes : examen des circuits clés et des montants supérieurs à un seuil de signification pour dresser des constats de carence et informer (résoudre) Obligation de moyens ?

Le contrôle de gestion

La distinction avec le contrôle de gestion (nous ne parlons pas ici du simple contrôle budgétaire) est la plus nécessaire car ces deux fonctions interviennent dans le même domaine, la gestion de l'entreprise et son amélioration, en fonctionnels (analystes, conseillers, d'ailleurs de formation similaire) et non en opérationnels (responsables, décideurs), et en toute indépendance (rattachement à haut niveau). Elles se distinguent par leurs modes opératoires.

Tableau 2.2 – Comparaison avec le contrôle de gestion

	AUDIT INTERNE Comment fonctionne ce qui existe ? Comment l'améliorer ?	CONTRÔLE DE GESTION Où voulons-nous aller ? Par où passer ?
Objectifs	Photo périodique et détaillée	Cinéma continu et global
Démarche	Va des problèmes rencontrés en pratique à leurs causes et conséquences	Va des indicateurs généraux aux paramètres particuliers
Rôle	Contrôle l'application des directives, la fiabilité des informations et l'adéquation des méthodes : les processus, les conditions d'obtention des résultats Audite la fonction contrôle de gestion	Planifie et suit les opérations et leurs résultats Conçoit et met en place le système d'information pour ce faire Analyse le budget du service d'audit interne
Horizon	Investigue le passé – seule réalité – pour trouver ce qu'on aurait pu faire de mieux et l'appliquer à l'avenir : semble vouloir changer le passé !	Pour maîtriser l'avenir (plan), analyse pourquoi le présent ne lui ressemble pas (écarts) : semble croire que le réel se trompe et que le plan a raison !
Mode d'intervention	Découvre les moyens organisationnels pour atteindre les objectifs Valide les objectifs (mode de détermination et faisabilité)	Élabore (mais ne décide pas) les objectifs en s'appuyant sur des hypothèses explicites Analyse coûts – bénéfices
Différences	Mécanicien de chaque secteur	Navigateur de l'ensemble des secteurs

La mission de l'audit interne et celle du contrôle de gestion se complètent et s'épaulent mutuellement :

- le contrôle de gestion peut demander un arrêt sur image, un zoom, une vue détaillée et sûre à l'audit interne (le navigateur peut demander au mécanicien de régler l'altimètre et le gyrocompas) ;
- l'audit interne peut s'appuyer sur la connaissance du contrôle de gestion pour élaborer le plan d'audit (le navigateur signale les turbulences).

Le risk management

L'audit interne et le *risk management* se complètent parfaitement lorsque les rôles respectifs sont bien définis, compris et admis par les deux parties.

En caricaturant, on pourrait simplifier en disant que par rapport aux risques, les uns (*risk managers*) en ont une vision « macro » et les autres (auditeurs internes) une vision « micro ».

Les *risk managers* sont les « experts » internes du risque. Ils les identifient, les classifient, les évaluent (impact/probabilité) et enfin élaborent les traitements à prévoir – acceptation du risque, recours à l'assurance, évolution du dispositif de maîtrise des risques.

Le *risk management* se situe en amont de l'activité d'audit interne, notamment dans la contribution qu'il peut apporter à l'élaboration du programme annuel d'audit par l'établissement d'une cartographie des risques, comme nous le verrons ultérieurement.

Tableau 2.3 – Comparaison avec le *risk management*

	AUDIT INTERNE	RISK MANAGEMENT
Cadres de référence usuels	COSO-I, COCO, cadre de référence AMF	Cadre de référence FERMA (<i>Federation of European Risk Management Associations</i>)
Cartographie des risques	L'exploite pour établir son programme annuel d'audit	En charge de l'établir
Par rapport au concept de risque	Expert de l'identification des risques spécifiques à chaque entité auditée	Expert de l'identification et de la quantification (impact/probabilité) des risques globaux
Mode d'intervention	Va sur le « terrain » et développe une méthodologie d'investigation détaillée	Intervient à distance et par un réseau de correspondants

La conformité (compliance)¹

Au cours des dernières années, la conformité et l'audit interne ont pris de l'importance, ces deux éléments représentant des composants de contrôle essentiels de la structure d'une organisation.

La fonction de conformité vise à garantir de manière raisonnable que l'entreprise respecte toutes les lois, règles et réglementations applicables, ainsi que les codes de conduite, politiques et procédures

internes. La fonction d'audit interne est conçue pour surveiller et évaluer l'environnement de contrôle interne de l'entreprise en ce qui concerne son adéquation, sa pertinence et son efficacité. Par conséquent, l'objectif de compliance est fondamentalement opérationnel : examiner le présent et l'avenir pour s'assurer que toutes les activités sont menées conformément aux exigences réglementaires en vigueur, car la politique et les procédures appropriées sont en place et sont respectées. L'objectif de l'audit interne est fondamentalement l'assurance : examiner le passé et le présent pour s'assurer que toutes les activités sont menées conformément à la politique et aux procédures écrites.

La conformité concerne le respect des obligations légales et réglementaires. Chaque organisation doit faire certaines choses pour s'assurer qu'elle se conforme aux lois, règles et règlements aux niveaux national et international. Si une organisation ne respecte pas ses obligations de conformité, elle peut être passible de lourdes pénalités telles que des amendes, voire des poursuites judiciaires et des atteintes à la réputation. La conformité des entreprises intègre également souvent les codes de conduite et la charte éthique d'une organisation. Ceux-ci peuvent indiquer comment les gens doivent se comporter et ce dont l'organisation a besoin pour fonctionner efficacement. La conformité est un processus continu qui devrait toujours être ouvert à l'amélioration et modifié chaque fois que les lois et les réglementations l'exigent. La conformité fonctionne souvent à tous les niveaux de l'entreprise, de la direction à l'atelier. Bien que des éléments importants de son rôle soient stratégiques, la conformité doit également être pratique pour trouver des solutions aux problèmes. Sans une connaissance détaillée de l'entreprise, les fonctions de conformité ne peuvent pas aider l'organisation à identifier le meilleur moyen de respecter ses obligations. Le responsable de la conformité doit être au courant des lois en vigueur et des lois en évolution potentiellement imposées par les organismes de réglementation. Ceci afin de définir la politique et les procédures opérationnelles à suivre par les parties concernées au sein de l'entreprise ou liées à l'entreprise, afin de se conformer et d'éviter tout risque potentiel autour de cela.

Rôle des deux fonctions dans la défense à trois lignes de la gouvernance d'entreprise

La fonction de conformité joue principalement un rôle de défense de second rang au sein de la gouvernance d'entreprise, mais elle a également une place dans la première ligne de défense pour ses propres activités pour évaluer, contrôler et atténuer les risques directement. Dans ce rôle, la fonction de conformité est chargée de surveiller divers risques spécifiques, tels que le non-respect des lois et réglementations applicables.

L'audit interne joue un troisième rôle de défense dans la gouvernance d'entreprise, qui est plus indépendant que les deux autres lignes de défense. Il fournit l'assurance indépendante du processus et du contrôle en place non seulement à propos du propriétaire du processus final, mais également de la seconde vie de la fonction de gestion des risques de la défense.

Enfin, la fonction de conformité ne concerne que le risque réglementaire et la portée des opérations est donc plus limitée que celle de la fonction d'audit interne, qui se préoccupe de tous les risques pour l'organisation.

Collaboration entre professionnels de l'audit et de la conformité

Les deux fonctions doivent travailler en coopération. L'audit et la conformité – travaillant ensemble – occupent une position privilégiée pour aider le conseil d'administration et la direction à comprendre l'importance d'une approche intégrée des activités de gouvernance qui permet une utilisation rationnelle des ressources, évite les résultats indésirables et exploite les avantages permettant d'atteindre les objectifs de l'entreprise.

Toutes les organisations doivent s'efforcer de former une équipe coopérative afin de fonctionner sans heurts. Le responsable de la conformité devrait idéalement travailler de manière intrinsèque au sein de l'organisation afin d'éduquer et de conseiller sur la conformité opérationnelle. Tous les membres de l'équipe doivent être conscients de leur rôle en matière de conformité par le biais d'une communication claire. Pour assurer une coordination efficace des activités entre ces deux fonctions, il est essentiel que celles-ci tirent parti d'un langage

commun de risque et de contrôle. Lors de l'audit d'une organisation, les domaines dans lesquels les obligations de conformité ne sont pas remplies peuvent être identifiés car ils représentent des risques importants pour l'entreprise.

Il y a cependant quelques différences intéressantes à noter :

- alors que le responsable de la conformité et l'auditeur doivent effectivement travailler en coopération, un auditeur doit rester totalement indépendant afin d'évaluer les procédures et de fournir une assurance sans préjugé ;
- le responsable de la conformité peut être audité par l'auditeur afin de s'assurer qu'il agit correctement, mais cela ne fonctionne pas dans le sens inverse. Cela est dû au fait que le rôle du responsable de la conformité est spécifique aux risques opérationnels et réglementaires et que le rôle de l'auditeur couvre tous les risques pour l'organisation.

Tableau 2.4 – Comparaison avec la conformité

	AUDIT INTERNE	CONFORMITÉ (COMPLIANCE)
Périodicité	Périodique	Permanent
Rattachement	Direction générale	Direction générale
Objet	Organisation, conformité, états financiers et performance	Concerne le respect des valeurs éthiques, obligations légales et réglementaires
Référentiels	Normes IIA et ISA Développe une méthodologie d'investigation détaillée	FCPA, loi Sapin 2 et autres réglementations externes
Produits finis	Recommandations	Carte des risques et plan d'actions/surveillance
Métiers	Auditeur	<i>Compliance officer</i> et manager

La protection des données personnelles

Devenu obligatoire depuis le 25 mai 2018, le RGPD (Règlement général sur la protection des données) ne trouve pas encore sa place dans toutes les organisations. Ce dispositif constitue pourtant un enjeu majeur dans la protection des données. Dans un contexte où chacun est tracé sur la toile ou au travers du SI de l'entreprise dans laquelle il travaille, le RGPD vise à protéger les données personnelles, définies comme toute information se rapportant à une personne physique qui

permet de l'identifier directement ou indirectement (notion proche de celle du chemin de révision). Par exemple son nom, ses données de localisation, ou un ou plusieurs éléments spécifiques propres à son identité physique, etc. Le RGPD s'applique à toute organisation européenne, ou ciblant des résidents européens, qui traite directement ou indirectement des données personnelles.

L'idée générale est de prôner l'auto-responsabilisation des entreprises, ainsi que l'information et le consentement des utilisateurs. Le RGPD fournit également des outils juridiques permettant de récupérer les données et d'exercer des actions en responsabilité. Le RGPD est le changement le plus important en matière de protection de la vie privée et de protection des données ; il est en tête des classements des risques majeurs identifiés par les auditeurs. Face à cet enjeu de conformité, le rôle de l'audit interne est d'évaluer le niveau de conformité et la pertinence du programme interne de conformité au RGPD.

On retiendra que les entreprises se doivent de cartographier l'ensemble de leurs traitements de données à caractère personnel à la fois pour des raisons légales, de transparence et de bonne gouvernance. Lors de l'audit, il y a lieu de vérifier la qualité du registre des activités de traitement (inventaire des données, traitement de données exécutées, identification des données sensibles, objectifs recherchés par les traitements, traitements qui impliquent des tiers, transfert hors UE des données traitées...). L'auditeur devra s'assurer que l'utilisation de la donnée par le SI ne nuit pas, ni dans son usage ni dans sa finalité, à la personne physique : *profiling*, fichiers stockés en vue d'un usage non défini renseignant des données dites sensibles (race, religion, donnée biométrique, etc.). Pour ce faire, l'auditeur pourra s'adresser directement au délégué à la protection des données (DPO), s'il existe, mais également au représentant légal de l'entreprise et/ou de ses sous-traitants informatiques qui produisent aujourd'hui systématiquement un acte d'engagement RGPD (code de conduite ou certification).

Il est à noter que la donnée transférée hors de la communauté européenne est également très encadrée ; en pratique, la technologie *cloud* – parce qu'elle permet l'hébergement dans des *data centers* en particulier aux États-Unis – ne permet pas de garantir cette protection ; en effet par exemple, le Patriot Act américain autorise l'administration

à se saisir de ces données. En pratique, un utilisateur va très souvent consentir à ce que ses données soient utilisées, soit parce que les conditions générales qui lui sont exposées à l'ouverture de telle ou telle application sont difficilement lisibles (voir écrites en anglais), soit parce que l'usage de l'application elle-même lui est depuis longtemps indispensable (réseaux sociaux en particulier).

Au regard de la protection des données personnelles, la France – et plus globalement l'Europe – se distingue des autres pays en pointe en matière de *big data*. Ainsi les États-Unis (GAFA) ou la Chine (BATX) exploitent sans retenue les données personnelles en vue de *profiling* à des fins commerciales, sociétales, politiques ou autres. Comme souvent, cette intention louable va produire vraisemblablement un effet inverse à celui recherché. En effet, l'intelligence artificielle (IA) et le *machine learning* nécessitent pour être efficaces d'avoir accès à un nombre colossal de données. Les contraintes liées au RGPD risquent de nous disqualifier un peu plus dans la course à l'IA, d'autant que nos investissements sur le sujet sont déjà faibles au regard des principaux acteurs que sont les États-Unis et la Chine, qui sont libres de passer outre.

Focus

L'audit de la protection des données personnelles

Intervenants au sein du master « Audit et gouvernance des organisations » à l'IAE d'Aix-en-Provence, nous recommandons aux lecteurs de s'appuyer sur le mémoire de fin d'études consacré à « l'audit de la protection des données personnelles à l'aune du Règlement général sur la protection des données » rédigé par l'étudiante Nadège Rispoli, qui a été récompensée par l'IFACI comme lauréate du prix Olivier-Lemant 2018.

Tableau 2.5 – Comparaison avec la protection des données personnelles

	AUDIT INTERNE	PROTECTION DES DONNÉES PERSONNELLES
Périodicité	Périodique	Permanente
Rattachement	Direction générale	DSI et/ou direction juridique
Objet	Évaluer le niveau de conformité et la pertinence du programme interne de conformité au RGPD	Informier et conseiller Contrôler le respect du règlement et du droit national en matière de protection des données Piloter la conformité
Référentiels	Normes IIA/IFACI qui définissent la méthodologie d'audit	RGPD et autres réglementations externes
Produits finis	Recommandations	Cartographie des traitements, gestion des risques et plan d'actions, organisation des procédures internes et documentation, surveillance
Métiers	Auditeur	DPO (délégué à la protection des données)

La qualité

Encore faudrait-il savoir de quelle qualité on parle ! S'agit-il de la démarche qualité qui s'inscrit dans le cadre du déploiement des normes ISO 9000 (que les toutes premières versions de cette norme appelaient l'assurance qualité) ou des approches dites « qualité totale ou globale » (*Total Quality Management*) qui s'inspirent de modèles tels que les référentiels EFQM (*European Foundation Quality Management*), Balbridge aux États-Unis ou autre Deming au Japon ?

Si nous nous cantonnons plus particulièrement au système de management de la qualité (SMQ) relatif aux normes ISO 9000, sa première version date de 1987. Depuis, de nombreuses actualisations sont venues améliorer considérablement le concept qualité. D'une vision « très procédurière » des premières versions, nous en sommes maintenant (notamment avec la dernière évolution significative de la version v2000 et sa suivante) à une conception plus « moderne » de la qualité qui se préoccupe plus du fond (satisfaction des clients) et moins

de la forme. L'engouement des organisations pour la certification en témoigne.

L'ambiguïté ne se situe pas entre l'audit interne et la qualité mais entre l'audit interne et l'audit qualité (qui constitue une obligation de la norme ISO 9001). Si les finalités de ces deux métiers sont les mêmes (le « contrôle du contrôle »), les modes opératoires et l'organisation des missions présentent des différences significatives.

Tableau 2.6 – Comparaison avec la qualité

	AUDIT INTERNE	AUDIT QUALITÉ
Organisation du service	Service à part entière d'une organisation, identifié	« Corps d'auditeurs qualité » composés de personnes
Nature des missions	Conformité, efficacité, efficience	Une dominante conformité
Durée des missions	« Longues », quelques semaines	« Courtes », quelques jours
Normes « d'audit »	Normes professionnelles de l'audit interne	Normes ISO 10011
Objectifs prioritaires	Identifier des zones de risques non couvertes par des dispositifs de contrôle interne	Identifier des exigences de la norme ISO 9001 non satisfaites par les dispositifs du SMQ existants conduisant à la non-satisfaction du client

Sans porter de jugement trop hâtif sur « la meilleure formule » quant à la combinaison entre l'audit interne et l'audit qualité (deux services séparés, un seul service), une chose est certaine : ce thème mérite une réflexion car nous sommes convaincus que des synergies sont possibles, bénéfiques pour toute l'organisation, pour peu que les experts se rapprochent.

La fonction contrôle interne

Pendant des décennies, la pensée dominante en matière de contrôle interne préconisait de ne pas créer une fonction spécifique en charge de la conception et de la mise en œuvre des dispositifs appropriés de contrôle interne (exception faite des établissements financiers pour lesquels la réglementation bancaire en imposait l'existence, règlement CRBF 97-02) et d'en laisser la charge aux responsables opérationnels et fonctionnels. Cette position se justifiait par le souci que ces mêmes

responsables se sentent complètement concernés par cette dimension et s'approprient cette culture du contrôle en participant à sa conception et à sa mise en œuvre. Nous partageons toujours cette position.

Cependant, depuis l'avènement de nouvelles obligations légales, notamment la loi Sarbanes-Oxley aux États-Unis et à un degré moindre la loi de sécurité financière en France, certaines des sociétés concernées se sont organisées différemment. Après avoir fait appel à des cabinets externes lors de la phase d'implémentation de ces nouvelles obligations, elles se sont dotées de véritables services de contrôle interne dont le rôle principal est de veiller à la « bonne maintenance » du système et à son amélioration (optimisation des dispositifs tout en respectant les obligations légales).

Ces services maintenant bien installés disposent de moyens importants et conjuguent souvent leurs efforts avec des « correspondants contrôle interne » dans les directions opérationnelles et fonctionnelles. Cette formule, qui associe des « experts du contrôle interne » dans un service central et des correspondants proches du terrain pour ne pas déresponsabiliser les directions, nous semble correspondre à l'évolution nécessaire compte tenu de la place grandissante de cette dimension « contrôle » dans nos économies actuelles.

Les principaux domaines d'activité de cette fonction sont l'établissement des cartographies de risques et la sensibilisation au contrôle interne de l'ensemble des acteurs de l'organisation. Les réseaux de contrôleurs internes se développent et leur périmètre d'intervention dépasse maintenant largement les aspects comptables et financiers.

Tableau 2.7 – Comparaison avec la fonction contrôle interne

	AUDIT INTERNE	FONCTION CONTRÔLE INTERNE
Objectifs	Apprécie l'existence, la pertinence, l'efficacité des dispositifs de contrôle interne (processus de management des risques, de contrôle et de gouvernance)	Conçoit et met en place les dispositifs de contrôle interne
Mode d'intervention	Va sur le « terrain » et développe une méthodologie d'investigation détaillée	Intervient à distance et par un réseau de correspondants
Complémentarité	Ces deux activités, lorsqu'elles cohabitent, se complètent. L'une (contrôle interne) conçoit et met en œuvre le contrôle interne, l'autre (audit interne) en apprécie l'existence, la bonne application et l'efficacité	
Différences	Dispose de suffisamment de recul sur « l'opérationnel » pour donner une opinion objective sur le dispositif de contrôle interne	Conçoit et met en œuvre, donc est trop impliquée dans la mise en œuvre pour apprécier la « qualité » du dispositif qu'elle propose

Les consultants externes « experts »

Depuis le début des années 2000, les grands cabinets d'audit externe ont développé, parallèlement à leur activité traditionnelle de commissariat aux comptes, des prestations de services dans le domaine du management des risques, du contrôle interne et plus généralement de la gouvernance d'entreprise. Au départ, la mise en œuvre des dispositifs propres aux obligations de la loi Sarbanes-Oxley en a été indéniablement le fait déclencheur. Aujourd'hui on peut considérer que bon nombre des entreprises concernées par ces nouvelles obligations légales sont « en régime établi ». Néanmoins ces cabinets interviennent toujours dans les organisations dans ces mêmes domaines. Leurs contributions se situent à plusieurs niveaux :

- pour des organisations de taille moyenne non pourvues de service d'audit interne, ils peuvent réaliser en tout ou partie de véritables missions d'« audit interne ». On parlera alors d'externalisation de l'activité d'audit interne ;
- pour des plus grandes organisations, dotées d'un service d'audit interne, la direction de l'audit peut souhaiter adjoindre à une de ses équipes d'audit un spécialiste « expert d'un domaine précis »

dont il ne dispose pas dans son effectif (exemples : auditeurs des systèmes d'information, juristes, spécialistes de la fraude...) ;

- au niveau du management des risques, ils peuvent intervenir dans la réalisation d'une cartographie des risques ;
- enfin, en fonction des évolutions législatives et/ou réglementaires, ils peuvent être amenés à traiter des problèmes divers en matière de gouvernance d'entreprise (par exemple, 8^e directive européenne transposée en droit français concernant les nouvelles compétences des comités d'audit).

On confond parfois « expert » et « expérimenté » en oubliant que, dans l'expérience, ce qui importe est la variété des situations vécues et non le nombre de fois où l'on a répété la même chose.

L'expérience peut être un handicap pour les consultants : elle incite à adopter les solutions qui ont réussi dans le passé, alors que les environnements, les hommes et les techniques disponibles peuvent être différents. Par contre, grâce à leur réseau, ces cabinets disposent de toutes les compétences dans tous les domaines, luxe que ne peut s'offrir un service d'audit interne.

**Tableau 2.8 – Comparaison avec les consultants externes
« experts »**

	AUDIT INTERNE	CONSULTANTS EXTERNES
Objectifs de l'intervention	Mettre en évidence les problèmes puis ébaucher des solutions	On sait qu'on va réorganiser, on fait venir quelqu'un pour le faire
Conditions requises	Des généralistes (tous problèmes) étayant leurs affirmations (non-spécialistes)	Connaissance spécialisée des solutions au problème déjà bien identifié
Base du savoir-faire	Méthodologie d'investigation	Expérience accumulée
Utilisation du savoir-faire	Cohérence interne des processus et systèmes de gestion Pertinence par rapport aux buts et objectifs	Des solutions qui ont fait leurs preuves ailleurs Comparaison situation du client/ expérience accumulée
Client réel	Le groupe Et l'audit interne exige que les problèmes démontrés soient résolus	Le commanditaire Il reste propriétaire du rapport et en fait ce qu'il veut

Les « experts/organiseurs » internes

Dans toutes les grandes organisations, il existe des spécialistes de tel ou tel domaine de gestion qui, de par l'expérience acquise, détiennent un savoir-faire indiscutable. Qu'ils fassent partie d'un service *ad hoc* (anciennement dénommé « organisation ») ou qu'ils soient attachés à des services divers et affectés ponctuellement à des missions de réorganisation, ils n'en constituent pas moins un apport interne intéressant. Lorsque les auditeurs internes ont fini leur mission et préconisé leurs recommandations, les responsables audités peuvent trouver là une aide précieuse pour la mise en œuvre des plans d'action.

Tableau 2.9 – Comparaison avec les organisateurs internes

	AUDIT INTERNE	ORGANISATEURS INTERNES
Interventions	Courtes : quelques semaines, visant à améliorer (sans bouleverser) Peut déboucher sur une réorganisation pour résoudre un problème et atteindre un objectif clairement défini	Longues : plusieurs mois, consistant à (casser puis) refaire Doit commencer par un audit pour détecter les faiblesses de l'organisation existante et préciser les objectifs
Objectifs	Détecter et évaluer les risques et dysfonctionnements, en rechercher les causes, faire cesser ces causes	Concevoir, réaliser et mettre en place les moyens adaptés, pour le futur immédiat ou plus lointain
Méthode	Compare le réel à un référentiel très centré sur le contrôle interne Orienté charges, il repère plus facilement les sous-activités	Analyse les méthodes et outils de travail, analyse des temps plus que des montants Orienté flux, il repère plus facilement les goulots
Responsabilité	Laisse la décision et l'action aux audités Reste indépendant	Décide et agit avec les intéressés Est engagé.

L'inspection

Tableau 2.10 – Comparaison avec l’inspection

	AUDIT INTERNE	INSPECTION
Régularité/ efficacité	Contrôle le respect des règles et leur pertinence, caractère suffisant	Contrôle le respect des règles sans les interpréter ni les remettre en cause
Méthode et objectifs	Remonte aux causes pour élaborer des recommandations dont le but est d’éviter la réapparition du problème	S’en tient aux faits et identifie les actions nécessaires pour les réparer et remettre en ordre
Évaluation	Considère que le responsable, « le chef », est toujours responsable et donc critique les systèmes et non les hommes : évalue le fonctionnement des systèmes	Détermine les responsabilités et fait éventuellement sanctionner les responsables Évalue le comportement des hommes, parfois leurs compétences et qualités
Service/ police	Privilégie le conseil et donc la coopération avec les audités	Privilégie le contrôle et donc l’indépendance des contrôleurs
Sélection/ sélectivité	Répond aux préoccupations du management soucieux de renforcer sa maîtrise, sur mandat de la direction générale	Investigations approfondies et contrôles très exhaustifs, éventuellement sous sa propre initiative

Attention : dans les banques, le titre « inspection » ou « inspection générale » couvre une combinaison des deux métiers.

L’Essentiel

- Les attentes des parties prenantes à l’activité d’audit interne sont fortes. Qu’il s’agisse des directions générales, des présidents de comités d’audit, des membres de conseils d’administration ou encore des directeurs financiers, tous ces « clients » de l’audit interne souhaitent que son périmètre d’intervention intègre les thématiques liées à la stratégie de l’entreprise en se focalisant sur ses enjeux et risques cruciaux.
- L’audit interne doit participer à l’organisation des trois lignes de maîtrise des risques (managers et responsables opérationnels, fonctions support, audit interne). Pour ce faire, il doit encore plus se professionnaliser afin d’accroître sa valeur ajoutée.
- La profession d’audit interne doit être encadrée par des normes. Le Cadre de référence international des pratiques professionnelles (CRIPP) en est le garant.

1. Ressources bibliographiques : IFACI, *Audit, risques et contrôle – la conformité : une préoccupation majeure des dirigeants*, revue n° 1, 2015. Chomma Shikati, “Internal Audit and Compliance: the Difference”, <https://medium.com>, octobre 2017.

Chapitre 3

L'organisation de l'activité d'audit

EXECUTIVE SUMMARY

- L'audit interne est une fonction à part entière de l'entreprise, à ce titre elle doit être organisée.
- Une fonction bien organisée s'appuie sur un certain nombre de principes de base tels que :
 - son rattachement hiérarchique ;
 - une charte qui définit ses objectifs et son mode de fonctionnement ;
 - une saine gestion de ses compétences humaines ;
 - une politique de communication ;
 - des outils pour en mesurer la performance.
- Vous trouverez dans ce chapitre des illustrations de bonnes pratiques en la matière sur tous ces aspects appliqués à la fonction audit interne.

LE RATTACHEMENT DE L'AUDIT INTERNE

À qui l'audit interne doit-il être rattaché ? À la direction générale, au directeur administratif et financier ou à tout autre directeur ?

D'après Louis Vaur, président d'honneur de l'IFACI, l'audit interne doit « être rattaché à une personne ou instance dont l'autorité lui assure le plus large domaine d'investigations, la liberté de son opinion, et la considération adéquate de ses recommandations ». Pour répondre à l'exigence d'indépendance, le service d'audit doit être indépendant (voir normes 1100, 1110, 1111 et 2020).

Le rattachement hiérarchique à la direction générale ou au président du conseil d'administration semble correspondre à ces spécifications et la tendance actuelle le confirme. Ainsi ils ne sont pas tentés d'influencer les conclusions de l'audit interne ou leur formulation. Mais l'expérience montre que, quand l'audit interne dépend d'un autre directeur, il résiste le plus souvent à cette tentation. On notera que, très probablement pour des raisons réglementaires, le taux de rattachement hiérarchique de l'audit interne à la direction générale est plus élevé pour les secteurs bancaires et assurance que pour les autres secteurs d'activité. Le rattachement à tout autre directeur menace l'indépendance de l'audit interne, même si la charte spécifie que l'audit interne intervient dans tous les domaines. Comment sortir de ce dilemme ? Par un double rattachement – quotidien à un directeur et fonctionnel à un comité d'audit (ou ce qui en tient lieu) :

- un directeur pour assumer la responsabilité administrative et aider l'audit interne en cas de besoin ;
- un comité d'audit émanant du conseil d'administration dont le but est de protéger l'organisation contre les irrégularités que les mandataires sociaux pourraient commettre ou promouvoir, et de rassurer les actionnaires.

En complément aux enquêtes publiées régulièrement par l'IFACI, on retiendra le CBOK (*Common Body of Knowledge*) qui est une étude menée sur l'audit interne à l'échelle mondiale. Parmi les prises de position sur le rattachement de l'audit interne on retiendra également les suivantes.

Prise de position de l'IFA/IFACI sur le rôle de l'audit interne dans le gouvernement d'entreprise (mai 2009)

Description

Il existe deux principaux modes de rattachement de l'audit interne et c'est à l'entreprise de trouver la meilleure combinaison pour optimiser les avantages de ces deux schémas. Pour cela, l'IFA et l'IFACI recommandent que l'audit interne soit rattaché à la direction générale afin d'assurer l'efficacité opérationnelle et l'implication du management mais également qu'il soit en relation étroite et régulière avec le comité d'audit, ce qui favoriserait son indépendance et le rôle de surveillance du conseil. De plus, les relations entre l'audit interne et ses deux organes de rattachement au sein de l'entreprise doivent être clairement identifiées avec par exemple : la périodicité, les procédures mises en œuvre, le mode de présentation et de synthèse des constats de l'audit interne ou encore les modalités de suivi des recommandations.

Intérêts

Cette prise de position peut utilement guider les entreprises dans le choix d'organisation de leur service d'audit interne.

Prise de position de l'IFACI sur l'urbanisme du contrôle interne (octobre 2009)

Description

« Au cours des dix dernières années, les services d'audit interne ont considérablement renforcé leur rôle et leur positionnement. Ils sont aujourd'hui, comme l'ont révélé les enquêtes les plus récentes, rattachés le plus souvent à la direction générale ou à un membre du comité exécutif agissant pour le compte de la direction générale et non pour le compte de sa propre fonction. Rarement membres du comité exécutif, si ce n'est comme membres non décisionnaires, afin de préserver leur indépendance, les directeurs d'audit interne entretiennent de plus en plus souvent une relation étroite avec le comité d'audit ou le conseil d'administration. »

Intérêts

Cette prise de position met en évidence l'essor et la prise de conscience des entreprises sur l'importance d'un service d'audit interne. Elle souligne également l'attention et la mise en œuvre des

recommandations des instances comme l’IIA ou l’IFACI dans la mise en œuvre du contrôle interne et le déploiement d’un service d’audit interne dans les entreprises. En effet selon l’IFACI, une majorité des entreprises ont rattaché l’audit interne à la direction (application directe de la norme 1110). On peut conclure sur le fait que cette prise de position ne constitue pas une évolution sur le rattachement de l’audit interne mais plutôt une réaffirmation plus détaillée.

LA CHARTE DE L’AUDIT INTERNE

Pour jouer pleinement leur rôle et contribuer ainsi à l’amélioration de la performance d’un groupe, les équipes d’audit doivent respecter une éthique et informer l’ensemble des parties prenantes sur leurs objectifs et leurs méthodes. L’existence dans chaque organisation d’une charte d’audit interne le permet. C’est un document solennel, élaboré par le responsable de l’audit interne, approuvé par la direction générale (majoritairement) et par le conseil ou le comité d’audit (accessoirement). Les normes 1000 et 1010 précisent que la mission, les pouvoirs et les responsabilités de l’audit interne doivent être formellement définis dans une charte d’audit interne. L’IIA fournit sur le site de l’IFACI un modèle type. La charte doit garantir les conditions d’indépendance de la fonction et protéger les audités contre tout excès.

Elle couvre notamment :

- la nature des missions couvertes ;
- la programmation des missions et le rôle que peut avoir l’encadrement (la saisine de l’audit interne), ainsi que la compétence de l’audit interne (tous domaines ou exclusions éventuelles) ;
- le déroulement d’une mission, vu des audités ;
- le processus de validation des conclusions, la diffusion des rapports, la définition (donc la limitation) du droit de réponse ;
- les responsabilités : les avis et recommandations de l’audit interne ne déchargent en aucune façon les personnes de l’organisation

auditée des responsabilités qui leur sont assignées ;

- le processus de suivi des recommandations ;
- les points majeurs de déontologie :
 - auditeurs : indépendance (l'auditeur n'a ni responsabilité, actuelle ou récente, ni autorité, actuelle ou prochaine, à l'égard des activités qu'il audite), droit d'accès, devoir de réserve, évaluation des systèmes et non des personnes ;
 - audités : devoir de communication, droit à la protection (validation avant diffusion, dossiers d'audit protégés).

L'auditeur doit être vigilant face aux travaux qui l'écartent de sa mission habituelle de contrôle. Ces demandes peuvent diminuer son efficacité et nuire à son indépendance de jugement. La charte peut alors être présentée comme une référence à respecter pour éviter d'éventuels dysfonctionnements. Il s'agit d'encadrer le pouvoir pour éviter toute apparence d'arbitraire. La charte fournit un support de communication de l'audit interne vers ses partenaires.

Focus

L'audit interne suit une procédure formalisée : la charte

L'audit interne (AI) intervient sur et uniquement sur mandat de la direction générale :

- « uniquement sur » : pas d'arbitraire ;
- « sur mandat » : l'AI a accès à tout document, fichier, installation, personne dès lors qu'il est mandaté.

L'auditeur est comme assermenté dans ses constatations et les auditeurs sont tenus au devoir de réserve. Leurs dossiers ne sont pas accessibles.

L'AI n'émet pas de commentaire sur les personnes. Ce sont les situations et les systèmes qu'il évalue.

Les conclusions de l'AI font l'objet d'un rapport écrit :

- un projet de rapport est validé avec les seuls intéressés avant d'être diffusé (procédure contradictoire) ;
- les éventuels désaccords des audités sont annexés au rapport (procédure écrite) ;
- le rapport définitif est ensuite diffusé aux responsables audités pour action et aux directions pour information.

L'AI recommande des solutions mais ne les décide ni ne les met en place. Ces recommandations ne déchargent en aucune façon le management de ses responsabilités.

L'ORGANISATION DES MOYENS

Il y a un côté physique dans l'audit interne : les déplacements et les nombreux dossiers, les observations de l'activité au petit matin et les inventaires le 31 décembre à minuit, mais c'est plutôt un travail intellectuel !

Les auditeurs doivent disposer d'un cadre de fonctionnement :

- le Cadre de référence international des pratiques professionnelles ;
- la méthodologie du service – elle est ce qui est commun à toute mission, elle guide l'élaboration de ce qui est spécifique à une mission donnée ;
- les documents et procédures de fonctionnement du service.

Il leur faut aussi des supports propres à chaque mission :

- « guides d'audit de... » décrivant une activité auditée, ses risques et ses pratiques d'organisation communément adoptées, incluant le tableau des risques, le programme de vérifications et l'état d'avancement final (base du prochain planning) de la dernière mission. Tant qu'on n'a pas accumulé cette expérience, on s'appuiera sur des ouvrages et manuels de référence ;
- on peut aussi constituer des bases de données des risques et dysfonctionnements rencontrés, consulter le fonds documentaire de l'IFACI (notamment les mémoires d'étudiants) ou feuilleter des ouvrages professionnels en librairie ;
- ne pas oublier la méthode la plus répandue pour pallier son ignorance : copier ceux qui savent. Outre les échanges d'expériences par le biais de l'IFACI, ce sera :
 - l'emprunt de personnel de l'entreprise compétent sur le sujet, pour participer à la phase d'étude, et éventuellement à l'analyse des constats (ou, plus limité, l'achat d'une expertise opinion réponse, externe ou interne, sur un point technique d'une mission) ;

- le transfert de technologie en effectuant une première mission conjointe avec un cabinet de conseil aguerri dans un domaine peu ou mal connu de l’audit interne.

Il faut enfin des outils informatiques : traitement de texte, tableur, logiciel de base de données, de présentations graphiques, de diagrammes de circulation, d’interrogation de fichiers. Apparaissent aussi des logiciels de gestion pour mener une mission ou pour élaborer le plan d’audit et suivre la mise en place des plans d’actions. En matière de recours à la sous-traitance (externalisation partielle ou totale de l’activité d’audit interne), on relève une faible proportion de cette pratique. Une minorité des services sous-traitent plus de 30 % de leur activité.

Prise de position de l’IIA sur les ressources de l’audit interne

Description

La problématique des ressources disponibles pour la fonction d’audit interne peut se poser en termes d’acteurs pour un besoin de compétences spécialisées ou des contraintes de délais, et de moyens pour des organisations de petite taille par exemple. Pour répondre à cette problématique, une organisation a la possibilité de faire le choix de l’externalisation partielle ou totale de sa fonction d’audit interne.

Dans les cas où celle-ci opte pour l’externalisation totale, l’IIA estime que la supervision et la responsabilité de l’activité d’audit interne ne peuvent pas être confiées au prestataire extérieur. Il convient de désigner un correspondant interne à l’organisation, de préférence un membre de la direction générale ou un cadre dirigeant, qui sera chargé de gérer l’audit interne externalisé. Si ce correspondant exerce par ailleurs d’autres responsabilités (hors audit interne), il conviendra d’évaluer les conditions relatives à son indépendance conformément aux normes des pratiques professionnelles. Lorsqu’il ne s’agit que de la sous-traitance d’une mission d’une courte durée, comme une mission spécifique ou une partie de mission, les auditeurs internes de l’organisation peuvent gérer et superviser la mission.

Intérêts

Étant donné l'importance de la fonction audit interne dans une organisation, lorsqu'elle est externalisée totalement ou pour une part significative, il y a lieu de confier sa responsabilité et sa supervision à un membre de la direction générale, ce qui permet de conserver la maîtrise des processus de gouvernance, de gestion du risque et de contrôle au sein de l'organisation.

LA GESTION DES AUDITEURS

La gestion du personnel de l'audit interne présente plusieurs particularités.

Les auditeurs sont organisés en pool

Les auditeurs sont en général organisés en un pool où l'on puise pour constituer les équipes : ils n'ont pas de lien hiérarchique permanent avec leur chef de mission sauf sur la durée d'une mission. La structure hiérarchique du service d'audit interne – quand il dépasse une personne ! – est :

- à deux niveaux dans les services de deux à cinq personnes (non compris le secrétariat) : « auditeurs » et « chef du service d'audit interne » ;
- à trois dans ceux de six à vingt personnes : « auditeurs », « chefs de mission », « directeur de l'audit interne ».

Dans les plus gros services apparaissent un quatrième niveau et souvent une décentralisation de l'audit interne. Nous nous placerons dans le cas de trois niveaux, pour distinguer les rôles de chef de mission et de responsable de l'audit interne, sachant que dans les petits services le chef cumule les deux rôles.

Les auditeurs sont affectés à un chef de mission le temps d'une mission, et pas forcément au même pour la suivante. C'est une des raisons de l'appréciation systématique à l'issue de chaque mission. Ils sont en général polyvalents (ou appelés à le devenir), sauf quelques

spécialistes de disciplines réputées difficiles et techniques. Dans les gros services, et notamment les entreprises multisecteurs ou multi-implantations (dont multinationales), on les regroupe par secteur ou région. Un auditeur est normalement affecté à une seule mission à la fois.

Les chefs de mission sont les piliers de l'audit interne. Leur rôle est d'animer et contrôler la progression des travaux, d'assurer leur qualité, et d'assumer l'interface avec les audités. Ils sont responsables du succès de la mission, vis-à-vis du service d'audit interne et vis-à-vis des audités. En principe, on est auditeur ou chef de mission selon les besoins, les spécificités et l'expérience requise : tantôt l'un, tantôt l'autre. Mais il y a souvent un « effet de cliquet », ne serait-ce qu'à cause de la rapide rotation des auditeurs et donc de la faible expérience de la plupart d'entre eux. Il est plus efficace qu'un chef de mission soit sur une seule mission à la fois. Il est parfois nécessaire qu'il en conduise plusieurs de front.

Poste tremplin ou fonction pépinière, on les embauche pour le poste suivant autant que pour l'audit interne. Dans 50 % des services d'audit interne, les auditeurs ont moins de quatre ans d'expérience en audit, et très peu ont plus de dix ans d'ancienneté. On les recrute pour le poste, mais ils viennent pour les perspectives, l'audit interne attire en tant qu'accélérateur de carrière. Il faut donc pouvoir faire état des bonnes sorties de leurs prédécesseurs, savoir quels sont les besoins de l'entreprise à moyen terme, et faire rencontrer aux candidats des responsables de l'entreprise. En général, lorsque les auditeurs quittent le service d'audit interne, la majorité d'entre eux s'orientent vers la direction financière, puis vers le management opérationnel d'entités et ensuite vers des services support (ressources humaines, systèmes d'information, communication...). Recrutements et sorties du service sont ainsi liés. Cela rend nécessaire une coopération étroite avec la DRH :

- à l'embauche, pour qu'elle décrive les besoins prévus, évalue les candidatures externes (son rôle habituel) et internes (aider à « lire » les dossiers)... et n'affecte pas le niveau de professionnalisme ;

- à la sortie pour qu'elle identifie des postes opportuns pour les intéressés, utiles à l'entreprise et promoteurs pour l'audit interne ;
- et entre-temps pour d'une part organiser ces sorties (côté audit interne cela pourra influencer sur l'affectation des missions), et d'autre part protéger l'audit interne des prédateurs qui confondraient pépinière, où l'on attend que la plante soit mature, et vivier où l'on se sert : quand les auditeurs sont bons, ils attirent les convoitises !

Quant au recrutement lui-même, il suit le processus habituel à l'entreprise, complété de discussions entre candidats et auditeurs pour s'assurer que les candidats s'intégreront à l'équipe en place. Le salaire moyen des auditeurs internes est légèrement supérieur à 70 k€ par an, dans une fourchette allant de 40 k€ à plus de 140 k€. De plus, trois quart des auditeurs ont une rémunération variable équivalente à 10 % de leur revenu.

Les auditeurs sont évalués à l'issue de chaque mission

Les auditeurs sont donc évalués plusieurs fois par an. L'audit travaillant par chantiers, il est bien normal qu'on évalue les ouvriers et le conducteur des travaux à la fin de chaque chantier (surtout quand les ouvriers changent de conducteur à chaque chantier). Le but est qu'ils modifient leurs façons de faire, tant au plan de la technique qu'à celui du comportement. Il s'agit de faire adhérer les intéressés aux évolutions à entreprendre, bien plus que de déterminer une note comparative (augmentations) ou absolue (promotions). Pour cela il est commode d'utiliser les deux grilles suivantes, l'une pour la technique et l'autre pour le comportement, dont les particularités sont :

- de présenter un grand nombre de points concrets afin d'être le plus objectif possible (une liste préétablie), mais qu'on traite rapidement (pas de note précise mais une flèche : augmenter/maintenir/réduire) ;
- de mettre en évidence des demandes de modifications et non des jugements de valeur blessants (des flèches et non des notes ; associer une expression de satisfaction à une critique, au moins pour le premier tableau).

EXEMPLES

Grille 1 – Évaluation de la technique

Productions de l'auditeur	Qualité	Célérité	Précisions éventuelles
FAR	→	↗	

« Tes FAR (feuille d'audit et de recommandations) sont maintenant bonnes, continue, mais tu devrais pouvoir aller plus vite, accélère. »

« Tu travailles vite, bravo, il te reste à augmenter la qualité de tes comptes rendus de tests. »

Grille 2 – Évaluation du comportement

Humour	↘
--------	---

Il s'agit du comportement (et non du caractère), de l'image et des réactions que cela suscite.

« Réduis ton humour, cela blesse les autres » (et non : « tu es trop caustique »).

« Réduis tes initiatives, cela dérange le fonctionnement de » (et non : « tu es trop indépendant »).

« Prends davantage d'initiatives, tu es compétent » (et non : « tu es compétent mais trop passif »).

Des objectifs de progression personnelle

Les objectifs dont on convient avec les auditeurs sont des objectifs de progression personnelle : maîtrise de la méthodologie et comportement, tâches formatrices, contribution aux objectifs du service.

EXEMPLES

Maîtrise de la méthodologie et critères possibles

– Autonomie : ne plus attendre les programmes de travail mais les préparer ; agir le plus souvent sans demander au préalable l'avis du chef de mission (ou du responsable de l'audit interne pour un chef de mission).

– Qualité rédactionnelle : les rapports nécessitent peu de réécriture.

– Capacité de synthèse et d'appréciation des enjeux : le lecteur du rapport ne met plus d'annotations du type « quel est le problème ? ».

– Des réunions ni soporifiques ni dégénérant en affrontements.

Tâches formatrices

– Un confirmé se met en tandem avec un débutant.

- Un débutant se familiarise avec un secteur de l'entreprise.
- Mettre à jour le programme de vérifications à l'issue d'une mission.
- Un cadre expérimenté débutant en audit revisite les référentiels d'audit existants...

Contribution aux objectifs du service

- Tirer le bilan de l'année.
- Réduire les délais de sortie.
- Auditer de nouveaux domaines ou d'une manière plus opérationnelle...

LA NÉCESSITÉ DE SE FORMER

La formation et le transfert d'expérience tiennent une très grande place dans le métier. L'auditeur doit consacrer chaque année entre cinq et dix jours à la formation.

Outre les formations universitaires diplômantes spécialisées en audit (notamment celles dans lesquelles nous enseignons) et les programmes de perfectionnement des grandes écoles, l'IFACI accompagne le développement des professionnels en offrant un catalogue riche de plus de 70 formations personnalisables. Il propose ainsi un ensemble de solutions pour accompagner la professionnalisation des auditeurs et contrôleurs internes et permettre leur montée en compétence. L'IFACI est certifié ISO 9001 pour la conception et la réalisation des actions de formation inter- et intra-entreprises à l'audit et au contrôle interne. Outre les formations « catalogue », l'Institut propose des formations sur mesure, intervient en formation continue et développe une offre croissante de formations à distance.

À la formation traditionnelle, il faut ajouter les certifications et certificats individuels (voir au chapitre 2, la section consacrée à l'IFACI). Nous considérons dorénavant nécessaire pour les professionnels de l'audit d'aller chercher le titre d'auditeur interne certifié CIA qui est la seule certification reconnue à l'échelle internationale pour les auditeurs internes. Elle constitue la référence internationale et démontre les compétences et le professionnalisme des auditeurs internes. Le CIA atteste des aptitudes des auditeurs internes à jouer un rôle important dans leur organisation. Au terme du

programme, les candidats sortent enrichis d'une expérience pédagogique, d'informations et d'outils leur permettant de pratiquer l'audit interne de façon professionnelle dans tous types d'organisations ou d'environnements de gestion.

Par ailleurs, l'auditeur se forme à partir des éléments suivants :

- l'initiation aux métiers et méthodes spécifiques de l'entreprise ;
- les réunions du service où les missions sont présentées par les uns et discutées avec les autres ;
- le coaching et le tutorat, notamment la revue des travaux de l'auditeur par le chef de mission et par le responsable de l'audit ;
- l'affectation des auditeurs à une mission dans un domaine nouveau pour eux.

Focus

La certification CIA permet de :

- prouver sa maîtrise de l'audit interne et son professionnalisme ;
- renforcer sa crédibilité au sein de la profession et dans son organisation ;
- accéder à de nouvelles opportunités de carrière ;
- se distinguer de ses pairs ;
- développer ses connaissances des meilleures pratiques ;
- poser les fondements de l'amélioration continue de ses compétences et de sa promotion ;
- faire reconnaître ses compétences.

Le programme de certification CIA a évolué en 2019. En voici les grandes lignes.

Partie 1 – Concepts de base de l'audit interne

Fondamentaux de l'audit interne

Indépendance et objectivité

Compétence et conscience professionnelle

Programme d'assurance et d'amélioration qualité

Gouvernance, management des risques et dispositif de contrôle

Risques de fraude

Partie 2 – Pratique de l'audit interne

Gestion de la fonction d'audit interne

Planification de la mission

Accomplissement de la mission

Communication des résultats de la mission et suivi des actions de progrès

Partie 3 – Connaissances économiques nécessaires à l'audit interne

Connaissance de l'organisation et de son environnement

Sécurité de l'informations

Système d'information

Gestion financière

Vous trouverez au chapitre 7 deux exemples de fiches d'évaluation et de progression personnelle, l'une pour l'auditeur, l'autre pour le chef de mission.

LA COMMUNICATION DE L'AUDIT INTERNE

La communication de l'audit interne doit être précise, objective, claire, concise, constructive, complète et dans les temps.

En effet :

- la précision de la communication permet d'éviter les erreurs et les doubles sens sous-jacents à une notion ;
- une communication objective est juste, impartiale ;
- une communication claire permet d'être facilement comprise, n'emploie pas de vocabulaire technique et fournit les informations les plus significatives ;
- la concision permet d'éviter tous les points inutiles, toutes les constructions superflues ainsi que les mots inutiles ;
- la communication constructive est utile pour la conduite des améliorations là où elles sont nécessaires ;
- une communication complète permet de fournir l'essentiel de l'information sans manquements au public cible et inclut toutes les informations et observations significatives qui servent les recommandations et les conclusions ;
- une communication faite au bon moment est opportune et permet donc au manager de prendre les mesures nécessaires afin de mettre en place des actions correctives.

Distinguons plusieurs cibles : la direction générale et les membres du comité d'audit, les audités, l'ensemble du personnel, l'encadrement.

- Concernant la direction générale et les membres du comité d'audit : les médias sont le résultat des enquêtes de satisfaction post-audit et la qualité du résumé ou de la synthèse de chaque rapport.
- Vis-à-vis des audités : on effectuera des présentations de la charte sur diapositives pour la réunion d'ouverture/d'installation de l'équipe. On diffusera la charte sous une présentation attrayante.
- Pour l'ensemble du personnel : les médias pourront être les journaux de l'entreprise, des vidéoclips, des journées portes ouvertes. Le contenu :
 - la charte et la promotion du contrôle interne : c'est la raison d'être de l'audit interne ;
 - les relations avec les audités : c'est ce qui les intéresse ;
 - la vie du service d'audit et la journée d'un auditeur (interview de l'auditeur) : c'est simple, parlant et sympathique ;
 - des *success stories* de missions ; c'est concret. Attention à choisir des sujets positifs (éviter les réductions des effectifs et détections de fraudes) ;
 - un message à faire passer : l'audit interne, une opportunité à saisir pour apprendre, servir et accélérer sa carrière.
- Vers l'encadrement, le message est plutôt : l'audit interne, une opportunité à saisir pour sécuriser le fonctionnement et améliorer les performances. Les moyens et méthodes (outre les précédents) :
 - participation aux stages que suivent les managers (école de guerre) ;
 - diffusion d'une synthèse des faiblesses relevées, rendues anonymes, pour que tous apprennent des erreurs de chacun ;
 - développement de check-lists de *self audit*.

Mais n'oublions pas la communication involontaire, celle qui vient de la réalité non fardée ; celle qui résulte du comportement des auditeurs en mission et du bouche-à-oreille, de la qualité du travail, du

ton des rapports et celle que répercutent les anciens auditeurs et stagiaires qui ont essaimé vers d'autres services de l'entreprise.

La mise en place d'un plan de communication (cibles, attentes, messages à faire passer, supports de communication) est souhaitable. Il permet une meilleure appréhension et compréhension de l'audit interne par ses « clients » grâce à une communication sur mesure pour chacun d'entre eux. L'efficacité de l'audit interne en est optimisée et par extension l'environnement de contrôle en est bénéficiaire. On relèvera parmi les prises de position sur la communication de l'audit interne les éléments suivants.

L'augmentation de l'utilisation de l'intranet comme média de communication

Description

À travers l'intranet de l'entreprise, l'audit interne peut mettre à disposition de l'ensemble des employés diverses informations telles que : la charte d'audit, la présentation de l'équipe, le réseau des anciens auditeurs internes, l'arrivée d'un nouveau manager, la certification...

Intérêts

L'intranet est un média qui permet de communiquer de manière directe avec l'ensemble des employés. Ceci permet une communication en dehors des périodes d'audit.

La mise en place de référents au sein de l'audit interne

Description

Des membres du service d'audit interne sont en charge de plusieurs processus, ils sont donc nommés référents. Ils doivent, avec les fonctions *corporate* concernées, développer et communiquer les connaissances et réflexions sur des sujets d'actualité. Cela peut prendre forme à travers la mise à jour des programmes de travail,

l'organisation de rencontres régulières (convention, séminaire de formation).

Intérêts

Cette pratique permet à l'audit interne de se créer un réseau avec des services en dehors d'une mission d'audit spécifique. Par conséquent, la visibilité des auditeurs internes en est accrue. C'est aussi un moyen de donner une image plus « participative » à l'audit interne. De plus, c'est un moyen de maintenir une actualisation des connaissances et compétences des auditeurs.

LES MESURES DE SATISFACTION ET DE PERFORMANCE DE L'AUDIT

Pour améliorer la qualité, les performances et l'efficacité d'une fonction ou d'une unité, outre l'introspection que peuvent mener ses membres, notamment son responsable, il existe trois méthodes : le *benchmarking*, les enquêtes de satisfaction des clients et l'audit de l'audit interne.

Qu'en est-il pour l'audit interne ?

Le *benchmarking* doit en général transiter par un tiers pour préserver l'anonymat du questionneur et des questionnés, et se distinguer de l'espionnage industriel. C'est le rôle des consultants en audit interne (et des relations à l'intérieur de l'Institut français de l'audit et du contrôle internes). La profession a été longtemps réticente aux enquêtes de satisfaction des clients : « L'audit n'est pas une lessive ! », « Reconnaître la légitimité d'attentes obère notre indépendance ; de plus, ces attentes sont contradictoires, évolutives, parfois illégitimes », « La réponse sera biaisée par une mission qui s'est mal ou bien passée ou par prudence ». Ces réticences s'estompent : c'est un standard de l'IIA et il y a un effet d'émulation et de boule de neige. D'ailleurs les médecins sont jugés par leurs patients et les professeurs par leurs étudiants... et « je préfère l'apprendre avant

mon patron ! ». En effet, ces enquêtes constituent un outil de pilotage et de communication.

- *Outil de pilotage* : quelles prestations sont à améliorer, quels moyens à mettre en place ? D'où proviennent les réticences des audités alors que la mission a été techniquement correcte ? Le niveau de perturbation est-il supportable ? Le produit – rapport et recommandations – convient-il ? Il s'agit de détecter les motifs d'insatisfaction avant que les relations se dégradent, et de mettre fin aux incidents et aux « critiques souterraines ».
- *Outil de communication* : la DG voit que l'audit interne s'applique l'obligation de transparence ; les audités apprécient ce professionnalisme ; les chefs de mission ont enfin un outil de mesure du relationnel.

Il s'agit donc de questionnaires communiqués aux audités à l'issue de la mission et aux commanditaires réels et potentiels une ou deux fois par an (rien n'interdit de les faire remplir par les auditeurs pour comparaison !). Les questions doivent porter sur l'impact sur les clients, non pas sur son origine (analyse des méthodes ou de la méthodologie de l'audit interne). Vous trouverez au chapitre 7 un exemple de questionnaire de satisfaction post-audit.

L'audit de l'audit interne était peu pratiqué avant les années 2000, hors les services d'audit interne décentralisés par le service central. Après la publication en 2001 d'un nouveau cadre de référence professionnel, l'IIA a développé une méthode et un service de *Quality Assurance Review* qui fournit une évaluation professionnelle et indépendante, et l'IFACI est allé beaucoup plus loin en proposant une certification permettant de mettre en œuvre les préconisations des normes 1300 et 1312 concernant l'assurance qualité. L'IFACI a ainsi créé une filiale IFACI Certification afin de pallier le problème de compétences et d'indépendance, sur le modèle de l'IIA. Cette filiale offre trois audits et contrôles :

- *la certification*, qui se renouvelle tous les trois ans et permet d'obtenir un label qualité ;
- *la revue qualité*, d'une fréquence de cinq ans, qui délivre une opinion sur le niveau de conformité aux normes du service d'audit interne ; l'approche ne permet pas d'obtenir un « label » ;

- *la validation indépendante d'une auto-évaluation*, dont la fréquence est au minimum tous les cinq ans, qui se compose d'un processus détaillé et documenté d'auto-évaluation et d'une validation sur site, indépendante de cette auto-évaluation.

L'Essentiel

- L'audit interne a un besoin vital de communiquer avec toutes ses parties prenantes, plus que toute autre fonction d'une organisation. La fonction, rattachée à la direction générale qui est son premier « client », doit expliquer sans relâche son rôle de conseil auprès des audités sur le terrain.
- « Rassurer les directions générales sur le respect des règles fixées tout en aidant les managers audités à mieux maîtriser leurs risques » est le message à faire passer. La charte d'audit en est le support.
- Le recrutement et la formation des auditeurs internes et surtout leurs perspectives d'évolution sont des sujets extrêmement sensibles dont tout bon directeur d'audit interne doit se soucier. La relative brièveté du « passage à l'audit interne » au cours d'une carrière professionnelle est une spécificité (du moins française) de la fonction.

Chapitre 4

L'identification des besoins d'audit

EXECUTIVE SUMMARY

- Au sein d'une organisation, quels sont les processus, fonctions, filiales ou encore thématiques qu'il est souhaitable d'auditer en priorité ?
- Dans cette multitude de composantes de l'organisation, existe-t-il « un endroit où le feu couve » ? Comment l'intervention des auditeurs pourrait-elle en mesurer l'ampleur et éviter qu'il ne se « propage » ?
- Vous trouverez dans ce chapitre des outils qui permettent d'identifier ces besoins d'audit. La cartographie des risques et le plan annuel d'audit en constituent les éléments essentiels.

L'ÉLABORATION D'UNE CARTOGRAPHIE DES RISQUES

Que cette démarche soit réalisée par un service *risk management*, dont c'est le fondement même, par un service dit de contrôle interne ou encore par le service d'audit interne lui-même, elle n'en demeure pas moins l'étape centrale de l'identification institutionnelle des besoins d'audit d'une organisation.

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

Indépendamment des missions d'audit qui en découleront éventuellement ultérieurement, cette approche du contrôle de l'organisation par l'identification des risques auxquels elle est exposée permet par ailleurs de définir les dispositifs adéquats à mettre en place pour maîtriser ces risques.

L'approche que nous proposons ici relève plus d'une démarche qui incomberait à un service *risk management* dont c'est la vocation première, plutôt qu'à un service d'audit interne pour lequel une cartographie des risques ne représente que les prémices à la réalisation de missions d'audit ultérieures.

Cependant l'auditeur pourra aisément s'en inspirer en simplifiant les étapes, le degré de détail souhaité afin de rendre cette tâche compatible avec les contraintes de temps du service d'audit puisqu'il ne s'agit pas, rappelons-le, de sa mission première.

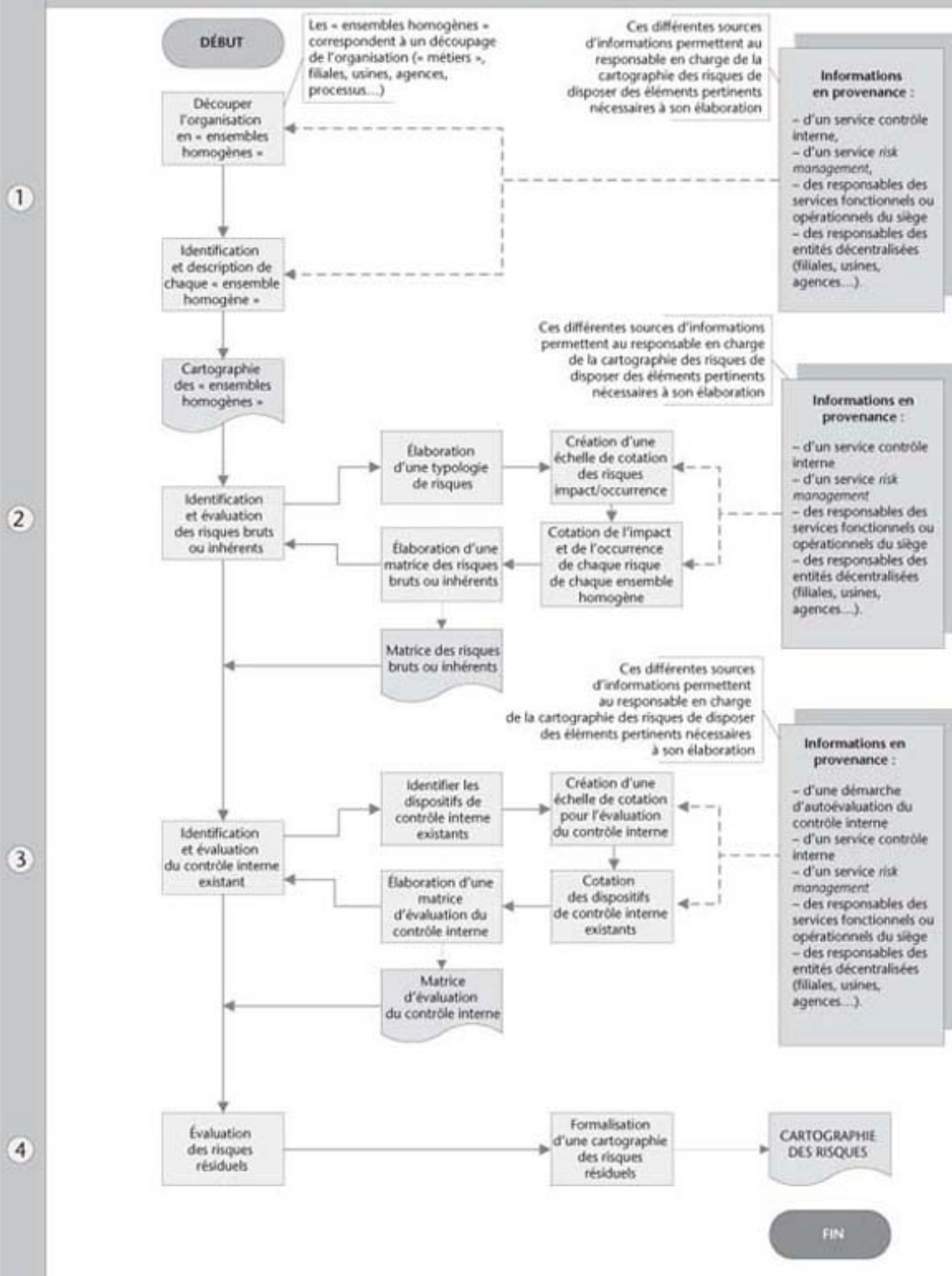
En matière d'élaboration d'une cartographie des risques, si les pratiques sont nombreuses, tout le monde s'accorde sur une logique partagée par tous les experts du management des risques.

C'est cette logique, socle commun en la matière, que nous présentons dans les schémas suivants. On y trouve les étapes classiques suivies dans l'élaboration d'une cartographie des risques.

- *Étape 1* : identification et description des « ensembles homogènes » (métiers, entités, processus) caractéristiques de l'organisation.
- *Étape 2* : identification et évaluation des risques inhérents ou bruts. Un risque est ainsi qualifié lorsqu'il est apprécié dans l'absolu indépendamment des dispositions existantes dans l'organisation pour en réduire l'impact et/ou la probabilité.
- *Étape 3* : identification et évaluation des dispositifs de contrôle interne présents dans l'organisation.
- *Étape 4* : évaluation des risques résiduels, c'est-à-dire ceux qui subsistent après la prise en compte de la dimension contrôle interne existante.

Identification des besoins d'audit : élaboration d'une cartographie des risques

Service en charge de l'élaboration de la cartographie des risques



Identification des besoins d'audit : élaboration d'une cartographie des risques

Tâches réalisées / responsables concernés

1 – IDENTIFICATION ET DESCRIPTION DES « ENSEMBLES HOMOGÈNES »

La première opération consiste à découper l'organisation en « ensembles homogènes ». Dans le cadre d'une organisation multi-activités, il est souhaitable de distinguer dans un premier temps les différents « métiers » de l'organisation, puis au sein de chaque « métier » les différentes « entités » (filiales, usines, agences...), enfin au sein de chaque « entité » les différents « processus » (achats, ventes, logistique, production...). En fonction du degré de précision souhaité de cette cartographie des risques, le découpage pourra évoluer d'un niveau très global « métiers », à un niveau intermédiaire « entités » à l'intérieur de chaque métier, ou encore à un niveau beaucoup plus détaillé « processus » de chaque entité à l'intérieur de chaque métier.

Pour chaque « ensemble homogène » il s'agit ensuite d'en obtenir une description (objectifs poursuivis, moyens alloués, volumétries...). Le responsable de cette démarche dispose de différentes sources d'informations pour réaliser cet inventaire (service contrôle interne, service risk management, responsables fonctionnels ou opérationnels du siège, responsables des entités décentralisées...). Cette première étape aboutit à l'élaboration d'une cartographie des « ensembles homogènes ».

2 – IDENTIFICATION ET ÉVALUATION DES RISQUES BRUTS

- * Élaborer une typologie de risques.
- * Définir une échelle de cotation des risques pour les deux paramètres caractéristiques : l'impact et l'occurrence.

Par exemple une échelle de 1 à 4 en fonction des critères suivants :

Échelle « impact »

- 1 Faible : pas de conséquences sur les valeurs, les objectifs stratégiques ou les actifs de l'organisation.
- 2 Modéré : risque présentant un impact surmontable.
- 3 Significatif : risque pouvant avoir un impact significatif sur les valeurs, les objectifs stratégiques ou les actifs de l'organisation.
- 4 Extrême : risque ayant un impact grave sur les valeurs, les objectifs stratégiques et les actifs de l'organisation.

Échelle « occurrence »

- 1 Faible : risque jamais apparu ou ayant une faible probabilité d'apparition.
 - 2 Peu probable : risque jamais apparu mais qui pourrait se manifester.
 - 3 Probable : risque apparu ou qui pourrait se manifester compte tenu du contexte.
 - 4 Très élevé : Très forte probabilité ou fréquence d'apparition.
- * Pour chaque « ensemble homogène » et pour chaque nature de risque, procéder à une cotation de l'impact et de l'occurrence.
 - * Formaliser les résultats dans une matrice des risques bruts.

3 – IDENTIFICATION ET ÉVALUATION DU CONTRÔLE INTERNE

- * Pour chaque « ensemble homogène » et au regard de chaque risque, identifier les dispositifs de contrôle interne existants.
- * Définir une échelle de cotation pour l'évaluation du contrôle interne par rapport à sa capacité de maîtrise des risques.

Par exemple une échelle de 1 à 4 en fonction des critères suivants :

- 1 Non maîtrise : absence de pilotage de l'organisation et de formalisation des procédures, compétences insuffisantes.
 - 2 Maîtrise partielle : pilotage empirique, esquisse de formalisation de procédures, compétences partielles.
 - 3 Maîtrise correcte : pilotage existant mais perfectible, procédures existantes mais perfectibles, compétences dans le domaine.
 - 4 Très bonne maîtrise : pilotage institutionnel performant, procédures rédigées, diffusées, appliquées et mises à jour régulièrement.
- * Procéder à une cotation des dispositifs de contrôle interne existants.
 - * Formaliser les résultats dans une matrice d'évaluation du contrôle interne.

4 – ÉVALUATION DES RISQUES RÉSIDUELS

En rapprochant, pour chaque « ensemble homogène », la matrice des risques bruts de celle concernant l'évaluation du contrôle interne, il s'agit maintenant de déterminer les risques résiduels. Un risque résiduel correspond à un risque brut non couvert (ou mal) par un dispositif de contrôle interne absent (ou défaillant).

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

Cette **CARTOGRAPHIE DES RISQUES** est un élément important pour l'identification des besoins d'audit lors de l'établissement du plan annuel d'audit.

Si nous avions voulu être tout à fait complets pour un expert en *risk management*, il aurait fallu ajouter à ces quatre étapes deux dernières préoccupations :

- *la phase de décision quant à l'acceptation du risque résiduel* ou la définition et la mise en œuvre de nouveaux dispositifs de prévention, de réduction ou de protection pour en assurer la maîtrise (assurance, dispositifs de contrôle interne...) ;
- *la mise en place d'un système de reporting* des résultats obtenus auprès de la hiérarchie concernée.

Enfin n'oublions pas que cette approche n'a de sens que si elle s'inscrit dans une démarche itérative. L'important n'est pas d'être exhaustif et pertinent « du premier coup », mais d'évoluer en permanence vers une « toujours meilleure maîtrise des risques » de l'organisation.

L'ÉTABLISSEMENT DU PLAN ET DU PLANNING D'AUDIT

Il s'agit d'identifier les besoins de l'organisation en ce qui concerne les ensembles homogènes (métiers, entités, services, processus) qu'il est souhaitable d'auditer en fonction des risques présumés de chacun d'eux (norme 2010 : planification du CRIPP). Toute la difficulté réside dans le fait d'estimer le niveau de risque de chaque ensemble homogène *a priori*, sans se rendre « sur le terrain ». Cette identification combine deux approches : l'une, pragmatique, intuitive, et donc subjective ; l'autre rationnelle, professionnelle, et donc intellectuelle. Chacune « borde » l'autre.

La première reconnaît que c'est aux dirigeants d'avoir la clairvoyance et d'assumer la responsabilité d'identifier les risques à auditer, l'audit interne ne pouvant être dans ce domaine, comme pour les recommandations en fin de missions, qu'un conseiller.

Pour cela, l'audit interne rencontrera les principaux dirigeants une ou deux fois par an et les experts chargés de l'identification ou de la

gestion des risques : où avez-vous des craintes et des incertitudes, qu'est-ce qui vous préoccupe ? Que pouvons-nous faire pour que vous puissiez « travailler sereinement », vous concentrer sur le cœur de votre métier ?

La seconde reconnaît qu'il faut aider les dirigeants à faire cela avec une approche raisonnée, que l'audit interne partage la responsabilité de couvrir les risques de l'organisation. Une démarche de cartographie des risques, précédemment définie, remplit cet objectif.

Nous n'insisterons jamais assez sur l'importance de cette étape d'identification des besoins. En effet le déséquilibre entre « les besoins d'audit » exprimés en nombre d'ensembles homogènes potentiellement auditables et les moyens (quantitatifs et qualitatifs) du service d'audit interne nécessaires pour les satisfaire est quasi permanent en ces périodes de restriction budgétaire. Il est donc primordial, pour une direction d'audit interne, d'être extrêmement vigilante à la bonne affectation de ses ressources.

Rien n'est plus consternant pour un « patron » d'audit que « d'envoyer ses troupes » auditer une entité sans enjeu majeur en matière de risque alors que dans une autre entité de l'organisation, oubliée dans le programme annuel d'audit, s'est déclaré un sinistre que « ses auditeurs » auraient pu prévenir.

Le résultat de la combinaison de ces deux approches sera discuté avec la direction générale (ou en comité d'audit) pour établir le plan de l'audit interne (norme 2020 : communication et approbation du CRIPP) : sûr à trois mois, prévu à six, probable à douze, indicatif au-delà.

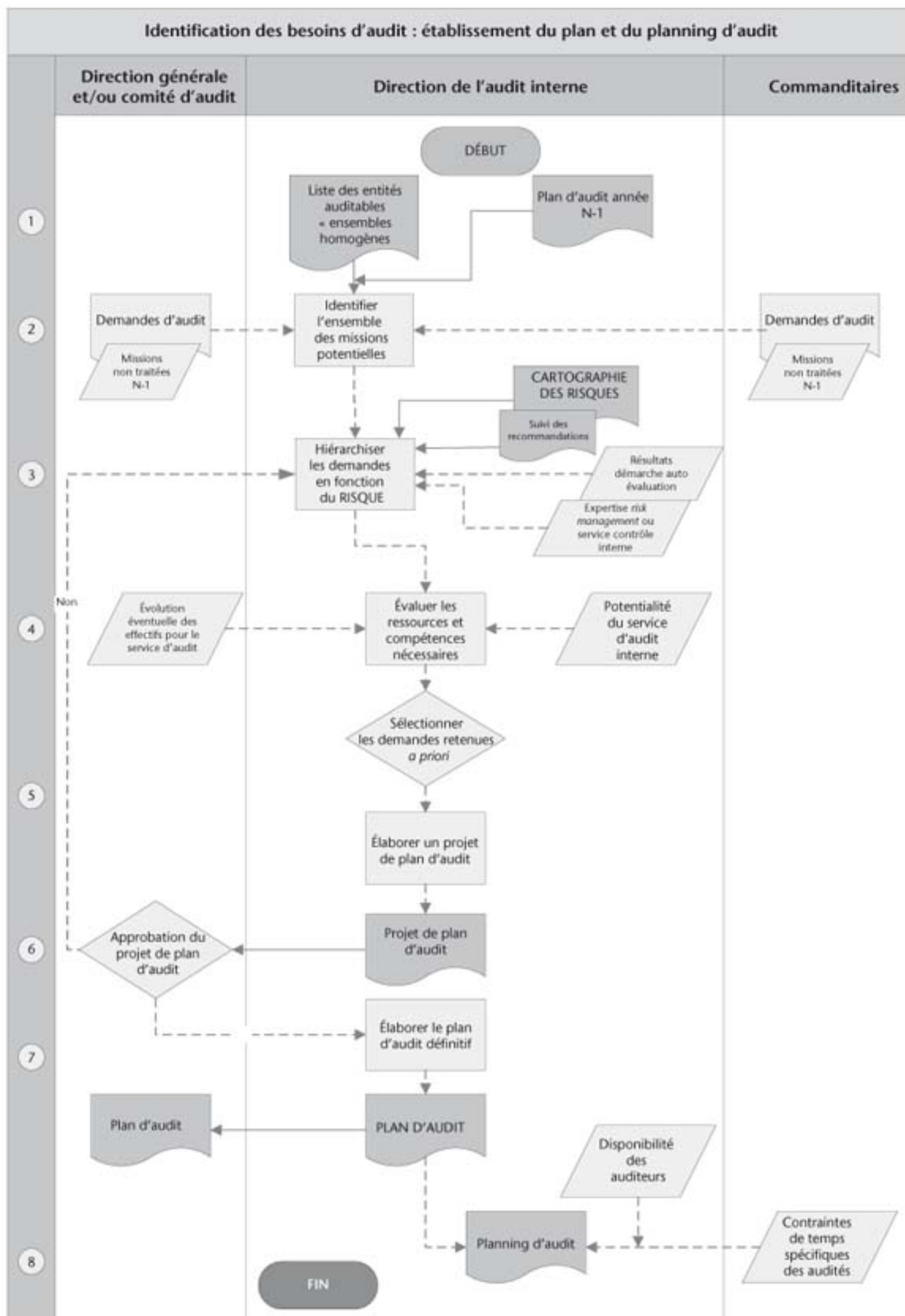
Ceci permet de prévenir les audités, et surtout d'informer les demandeurs de missions. C'est aussi le point de passage pour décider des ressources de l'audit interne, en quantité et en compétences (norme 2030 : gestion des ressources du CRIPP) – effectifs, profil des recrutements, formation – ou faire appel à des compétences extérieures.

Focus

Élaboration du programme d'audit

Les approches par une cartographie des risques et par les demandes spécifiques de la direction générale sont les critères majeurs permettant d'établir le plan d'audit.

L'approbation du plan d'audit est de la responsabilité de la DG et du comité d'audit.



Identification des besoins d'audit : établissement du plan et du planning d'audit

Tâches réalisées / responsables concernés

- 1 – Le responsable de l'audit interne liste tous les ensembles potentiellement auditables sur la période du plan d'audit. Si l'organisation dispose d'une cartographie des risques, ces ensembles auditables peuvent correspondre à la notion « d'ensembles homogènes » définie précédemment. Ce listing se doit d'être exhaustif, pour cela plusieurs approches permettent de cerner les missions possibles :
 - * Approche par « métiers » de l'organisation.
 - * Approche par « entités » : filiales, usines, délégations régionales, agences...
 - * Approche processus : audit du processus « achats », du processus « vente », du processus « gestion des stocks »...
 - * Ou encore approche thématique : audit de la sécurité, de la communication, de la politique de vente...
- 2 – Un audit mandaté par la direction générale revêt une importance particulière étant donné qu'il se place au sein d'une stratégie globale du groupe et doit être priorisé. Les audits demandés par la direction générale peuvent être :
 - * Des audits thématiques (politique environnementale...).
 - * Des audits stratégiques ou de performance.
 Les audits demandés par les autres commanditaires (directions opérationnelles ou fonctionnelles du siège, directions de filiales...) viennent compléter les demandes de la direction générale. Toutes ces demandes doivent être formalisées.
 La direction de l'audit interne, à partir de ces différentes sources d'informations, recense l'ensemble des besoins en termes d'ensembles auditables (métiers, entités, processus, thématiques).
- 3 – La direction de l'audit interne hiérarchise l'ensemble de ces demandes en fonction des risques spécifiques de chacune des entités potentiellement auditables. Pour cela il dispose de plusieurs sources d'informations :
 - * Les résultats d'une cartographie des risques.
 - * Les résultats d'une démarche autoévaluation.
 - * Les travaux d'un service « risk management » et/ou d'un service « contrôle interne » si l'organisation en dispose.
 - * Le suivi des recommandations des missions précédentes.
 Le responsable de l'audit interne en collaboration avec son équipe peut procéder à une pondération des risques. Cette pondération s'effectue selon plusieurs critères :
 - * Une appréciation quantitative du risque : évaluer le poids de l'entité auditable en fonction de son volume d'activité.
 - * Une appréciation qualitative du risque.
 - * Une appréciation *a priori* du contrôle interne existant dans l'entité auditable.
- 4 – Avant de sélectionner les entités auditées, la direction de l'audit évalue les ressources et les compétences dont elle dispose pour assurer le plan d'audit. Éventuellement elle sollicite des moyens supplémentaires auprès de la direction générale.
- 5 – En fonction des demandes préalablement hiérarchisées et des capacités d'intervention du service d'audit interne (effectif du service et compétences), le directeur du service d'audit interne sélectionne les demandes de missions à retenir dans le plan d'audit. Il élabore un projet de plan d'audit.
- 6 – Lorsque toutes les missions d'audit sont définies et priorisées, le plan d'audit doit être avalisé par la direction générale et/ou le comité d'audit (La 8^e directive européenne traduite en droit français rend obligatoire l'existence d'un comité d'audit en charge des problématiques de risques).
 Un plan d'audit est défini sur une période de 3 à 5 ans mais est revu annuellement et peut être modifié sous demande expresse de la direction générale et/ou du comité d'audit.
- 7 – Si le projet de plan d'audit n'est pas validé par la direction générale et/ou le comité d'audit, celui-ci est revu par le directeur de l'audit en tenant compte des nouvelles priorités fixées par la direction générale (étape 3). Si le projet de plan d'audit est validé par la direction générale et/ou le comité d'audit, le directeur de l'audit établit un plan d'audit définitif.
- 8 – En fonction des disponibilités des auditeurs et des contraintes de temps éventuelles des entités à auditer, le directeur de l'audit établit un planning d'audit précisant :
 - * La date de début et la durée probable de chaque mission.
 - * La composition de l'équipe d'audit.
 - * La date de remise du rapport aux audités.
 - * ...

L'Essentiel

- La cartographie des risques d'une organisation permet d'identifier les zones (processus, fonctions, filiales...) les plus exposées aux risques. Il s'agit d'un exercice difficile mais incontournable dans la perspective d'une bonne utilisation des ressources d'audit. Son élaboration nécessite une approche méthodique, participative, itérative et adaptée aux enjeux de l'organisation et à son exposition aux risques.
- Le programme annuel d'audit définit la nature des missions d'audit à réaliser, le planning d'exécution et les moyens nécessaires en termes d'auditeurs. Il se construit à partir de la cartographie des risques (approche méthodique) mais également en rencontrant les directions (générale, fonctionnelles et opérationnelles) de l'organisation. Cette seconde approche, plus pragmatique et intuitive, permet de « prendre le pouls » des dirigeants quant à leurs préoccupations en matière de risques.

Partie 2

La méthodologie de l'audit

[Les processus de conduite d'une mission Chapitre 5](#)

[Les modalités d'application \(MA\) Chapitre 6](#)

[Les documents associés \(DA\) Chapitre 7](#)

Chapitre 5

Les processus de conduite d'une mission

EXECUTIVE SUMMARY

- Trois grandes phases composent une mission d'audit : étude, vérifications et conclusion. Les normes professionnelles parlent de planification, accomplissement et communication.
- Elles sont décomposées en six processus définissant le déroulement d'une mission d'audit. Pour présenter chacun de ces processus, nous avons établi des schémas qui décrivent le cheminement des opérations à réaliser.
- Cette partie de l'ouvrage présente le diagramme global des étapes qui constituent une mission d'audit interne et une fiche explicative associée synthétise cette partie. Nous nous sommes placés dans le cas d'une mission nouvelle afin de détailler chacun des processus de conduite d'une mission.
- Un schéma précise, pour chacune des étapes, les références des normes professionnelles du CRIPP plus particulièrement concernées afin de faire un lien entre la méthodologie proposée et le cadre normatif international.

DIAGRAMME GLOBAL D'UNE MISSION D'AUDIT INTERNE

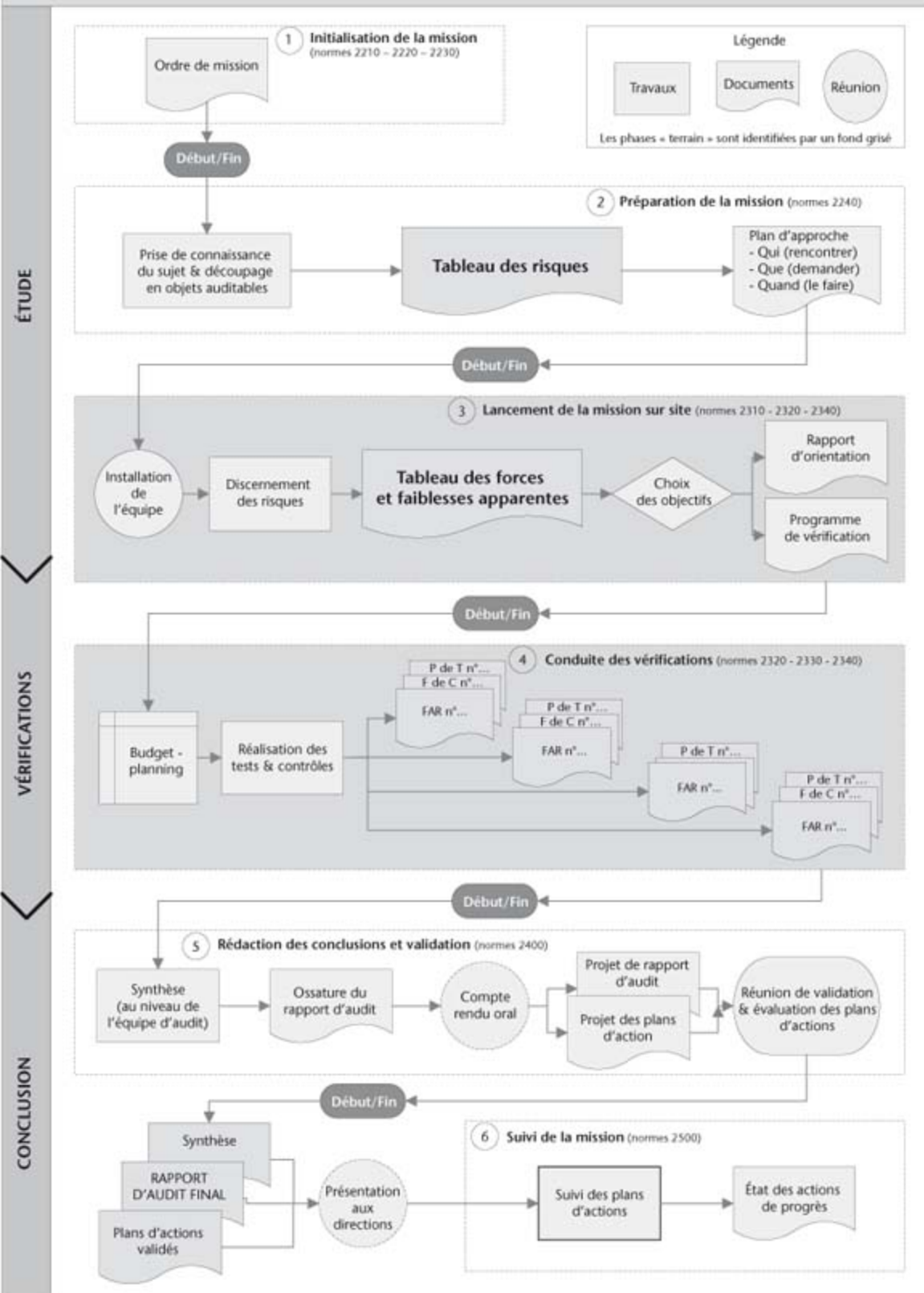


DIAGRAMME GLOBAL D'UNE MISSION D'AUDIT INTERNE

Début

1 - Initialisation de la mission (le droit d'accès ou l'ordre de mission)

L'équipe d'audit en charge de la mission doit se faire préciser clairement les attentes du (ou des) commanditaire(s). Elle établit pour cela un ordre de mission qui est validé par le commanditaire et présenté au(x) responsable(s) de l'entité auditée. Cet ordre de mission constitue à la fois le contrat passé entre le service d'audit et le demandeur de la mission et le droit d'accès de l'audit à l'entité concernée.

2 - Préparation de la mission (examen de l'activité et élaboration d'un Tableau des Risques - TaRi)

L'équipe d'audit établit le tableau des risques relatif au domaine audité (ou ajuste celui existant si le service d'audit interne dispose d'une « bibliothèque » de référentiels des risques). Un tableau des risques relate, pour une thématique donnée, les bonnes pratiques en matière de contrôle interne qui devraient être présentes dans l'entité objet de l'audit. Dans la suite de la mission, ce référentiel sert de base à laquelle « la réalité du terrain » va être comparée. C'est un document fondamental pour le bon déroulement de la mission et la qualité des conclusions de l'audit. Il sera revu par le chef de mission et présenté aux audités avant le lancement de la mission sur site.

3 - Lancement de la mission sur site (de la réunion d'ouverture au programme de vérification)

La réunion d'ouverture marque le lancement officiel de la mission d'audit dans l'entité concernée. L'équipe d'audit, en partant du tableau des risques préétabli, identifie durant cette phase les forces et faiblesses apparentes du contrôle interne de l'entité auditée. Cette démarche de discernement des risques se construit, par des entretiens avec les audités, la consultation de la documentation disponible concernant les processus... Un Tableau des Forces et faiblesses Apparentes (TFfA) synthétise ce travail d'identification des éventuels dysfonctionnements (et points forts) de l'organisation. Mais à ce stade tous ces éléments s'inscrivent dans un cadre théorique sans valeur probante. Dans la perspective de conduire des vérifications l'équipe d'audit établit, à partir du tableau des forces et faiblesses apparentes :

- Un rapport d'orientation qui définit les grands axes d'investigation pour la suite, destiné aux audités pour information.
- Un programme de vérifications, à usage de l'équipe d'audit et qui précise la nature des contrôles à réaliser.
- Un budget planning qui précise la répartition des contrôles dans le temps et entre les membres de l'équipe.

4 - Conduite des vérifications

Durant cette phase de vérification, l'équipe d'audit réalise l'ensemble des travaux de contrôle prévus au programme de vérifications. Pour ce faire les auditeurs disposent des techniques d'audit mises à leur disposition.

Afin de conserver la traçabilité des contrôles réalisés, ils formalisent tous ces travaux dans divers documents :

- Les « papiers de travail » véritables « brouillons » des auditeurs sur lesquels sont consignés le détail des investigations.
- Les « feuilles de couvertures » qui résument, pour chaque contrôle, l'objectif du contrôle, sa nature, les résultats obtenus et les conclusions de l'auditeur en charge du contrôle.
- Enfin, lorsqu'un contrôle atteste d'un dysfonctionnement, une Feuille d'Audit et de Recommandations (FAR) synthétise l'opinion de l'auditeur sur cette faiblesse de contrôle interne.

La FAR relate pour le problème évoqué les éléments de preuves qui en révèlent l'existence, les causes avérées, les conséquences réelles ou potentielles et enfin les propositions de recommandations formulées par l'équipe d'audit pour remédier à ce dysfonctionnement.

5 - Rédaction des conclusions (de l'ossature du rapport d'audit à sa validation)

L'équipe d'audit doit maintenant établir les conclusions de sa mission. Dans un premier temps à travers la construction de l'ossature du rapport d'audit qui va servir de support pour le compte rendu oral sur site auprès des audités et de base pour l'établissement du projet de rapport. Une fois validé par le chef de mission, ce projet de rapport est communiqué aux audités en préparation de la réunion de validation. Cette réunion est déterminante quant à la valeur ajoutée de la mission d'audit. Elle donne l'opportunité aux audités de demander des explications sur les dysfonctionnements révélés et contribuer à l'élaboration des recommandations définitivement retenues. Suite à cette réunion, les auditeurs établissent le rapport d'audit final communiqué au commanditaire et les audités finalisent leurs plans d'actions retournés au service d'audit afin de permettre le suivi de la mise en œuvre des recommandations.

6 - Suivi de la mission (le suivi des recommandations et les actions de progrès)

À des échéances bien précises après la fin de la mission (par exemple 3 mois, 9 mois, 1 an), le service d'audit a en charge le suivi de la mise en œuvre des plans d'actions afin de « boucler la boucle » et de remplir complètement et véritablement sa mission. Ce suivi peut prendre diverses formes (d'un simple déclaratif de la part des audités jusqu'à des missions d'audit de suivi de courte durée sur le terrain), il fait l'objet d'une transcription sur un « état des actions de progrès ». À l'achèvement de la mise en œuvre des plans d'actions, l'état final des actions de progrès est communiqué au commanditaire de la mission.

ÉTUDE

VÉRIFICATIONS

CONCLUSION

Fin



Le schéma précédent résume les grandes étapes détaillées dans les pages suivantes.

- **La phase d'étude** (Norme 2200 : Planification de la mission du CRIPP) se prépare au bureau (et dans les fonds documentaires) et s'effectue sur le terrain.
- **La phase de vérifications** (Norme 2300 : Accomplissement de la mission) est bien entendu totalement terrain.
- **La phase de conclusion** (Norme 2400 : Communication des résultats) est une alternance d'actions et d'interactions internes à l'équipe d'audit et avec les audités.

Les deux premières phases sont approximativement de même durée quand le sujet de la mission est nouveau – la phase de conclusion est plus courte – mais lorsque l'on dispose de programmes de travail rodés, la phase d'étude peut ne prendre que quelques journées. D'où l'utilité de capitaliser le savoir-faire du service.

Pour le responsable de l'audit interne, il s'agit de composer l'équipe, lancer la mission, encadrer l'équipe en phase d'étude, installer l'équipe, revoir les fiches d'audit et de recommandations (FAR) et la tenue des dossiers, suivre l'avancement de la mission et réagir, revoir le rapport (projet et définitif), présider la réunion de validation, surveiller le retour des réponses aux recommandations, veiller à la mise en œuvre des actions prévues. Plus globalement, il s'agit de suivre le budget (essentiellement les budgets de temps), bâtir des standards de temps, et accroître la productivité.

Six processus jalonnent le déroulement d'une mission d'audit interne et sont présentés ci-après sous forme de *flow chart*, outil bien connu des auditeurs :

I – L'initialisation de la mission : le droit d'accès ou l'ordre de mission.

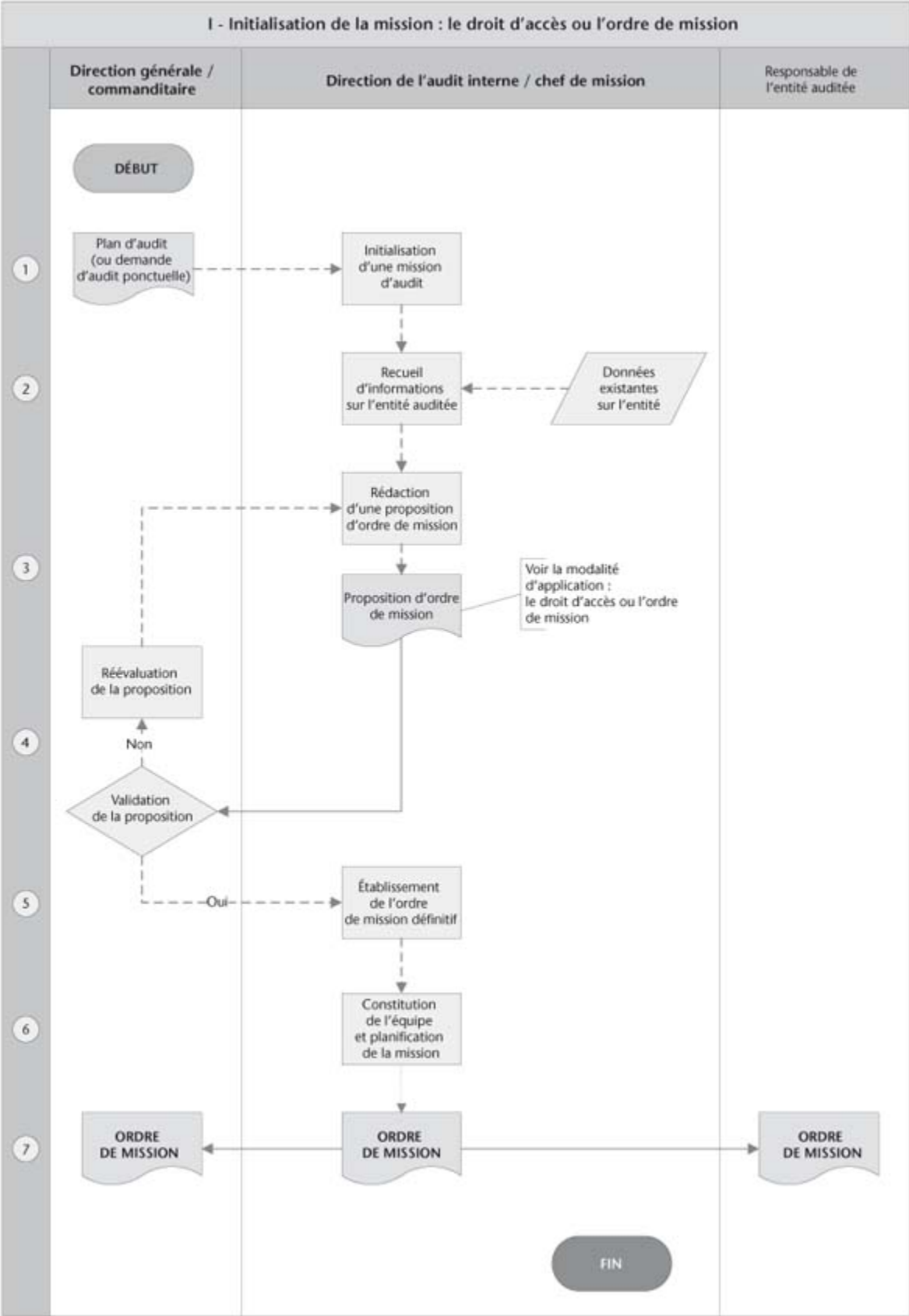
II – La préparation de la mission : l'examen de l'activité et l'élaboration d'un Tableau des risques.

III – Le lancement de la mission sur site : de la réunion d'ouverture au programme de vérification.

IV – La conduite des vérifications, de la feuille de couverture à la FAR.

V – La rédaction des conclusions : de l’ossature du rapport d’audit à sa validation.

VI – Le suivi de la mission : le suivi des recommandations et les actions de progrès.



I - Initialisation de la mission : le droit d'accès ou l'ordre de mission

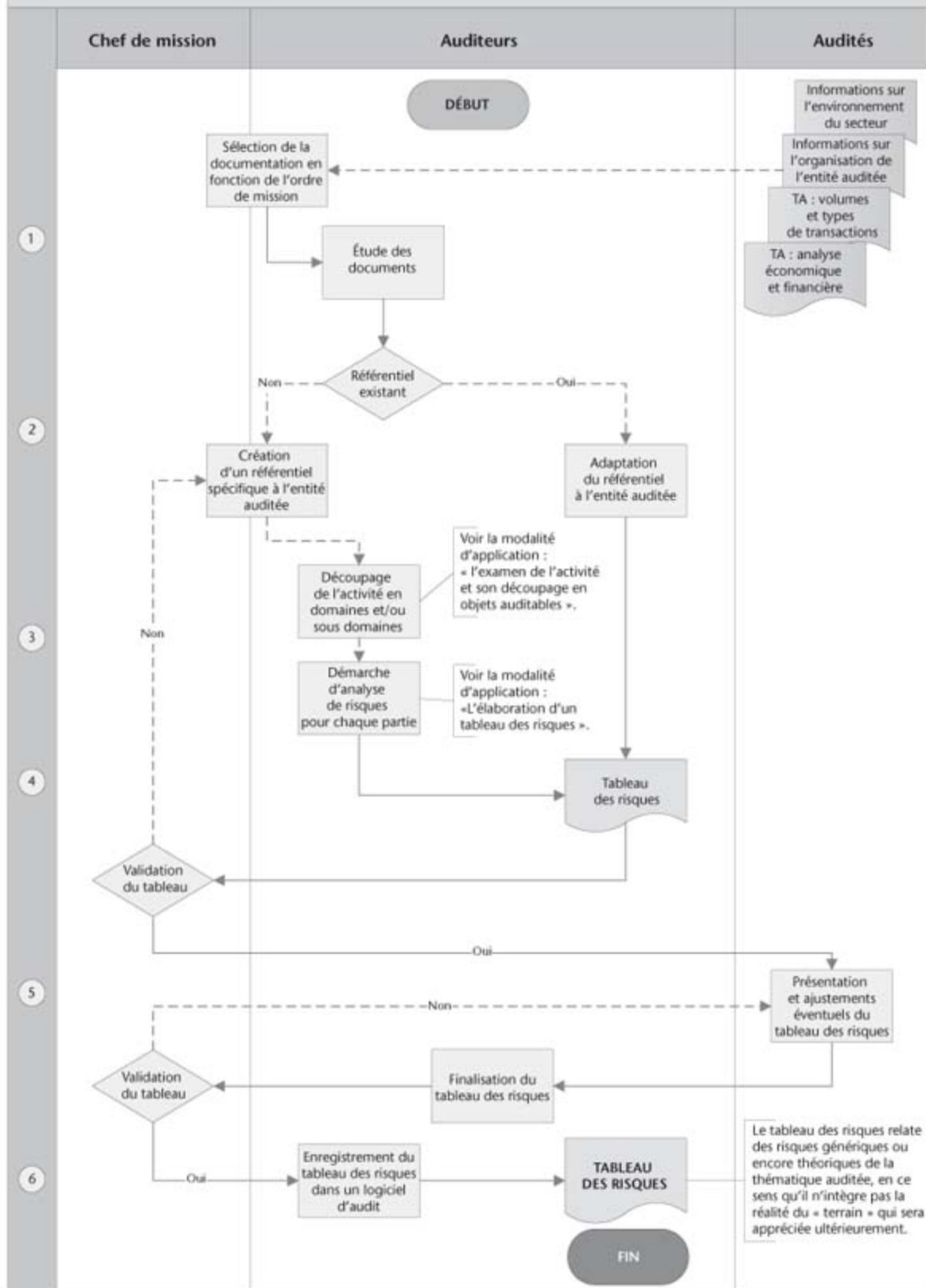
Tâches réalisées / responsables concernés

Modalités d'Application (MA) & Techniques d'audit (TA) & Documents associés (DA)

Voir MA : le droit d'accès ou l'ordre de mission

- 1 – L'initialisation d'une mission d'audit s'effectue à partir :
 - * Soit des besoins référencés dans le cadre du plan d'audit préalablement établi, et la demande est prise en compte définitivement.
 - * Soit des demandes ponctuelles en cours de période qui devront faire l'objet d'arbitrages. Dans ce cas, la demande doit être formalisée au travers d'une « demande d'audit » et validée par la direction générale. À ce stade, la mission est officiellement créée au niveau du service d'audit interne (par exemple initialisation dans un logiciel d'audit...).
- 2 – Dès la création de la mission, le chef de mission (CM) et/ou la direction d'audit interne (DAI) doit recueillir les informations nécessaires sur les activités à auditer en vue de la rédaction d'une proposition d'ordre de mission. Ces informations peuvent être de nature diverses : rapports d'audit précédents, documentation existante, tableaux de bord de gestion... Il peut également rencontrer le commanditaire de la mission afin de se faire préciser les attentes du demandeur (**TA : interviews**).
- 3 – Le CM (et/ou la DAI) établit l'ordre de mission. Un ordre de mission (DA : ordre de mission) doit comprendre :
 - * L'objet de la mission.
 - * Une brève description de la mission (champ, objectifs généraux attendus, points prioritaires).
 - * La date de début et la durée prévisionnelle de la mission.
 - * Le(s) demandeur(s).
 - * Les destinataires.
- 4 – Chaque ordre de mission d'audit doit ensuite être validé. En effet l'audit interne ne décide pas de lui-même. Si la proposition d'ordre de mission n'est pas validée, celle-ci peut faire l'objet d'un ajustement afin de mieux correspondre aux attentes.
Il peut :
 - * Demander une réévaluation du champ de la mission.
 - * Exprimer un changement dans ses attentes qui influera sur les objectifs de l'audit.
 - * Demander à revoir la période de mission.
 - * Prendre en compte les attentes d'un nouveau demandeur.
- 5 – La proposition d'ordre de mission devient un ordre de mission définitif une fois approuvée par le commanditaire. L'ordre de mission constitue alors un mandat de la direction générale.
- 6 – En fonction de l'ordre de mission et du planning d'audit, la DAI accrédite une équipe pour la mission et fixe les dates définitives de celle-ci en concertation avec le commanditaire et les audités.
- 7 – L'ordre de mission est ensuite communiqué avant le début effectif de la mission au commanditaire et aux responsables audités. Un ordre de mission constitue le véritable point de départ de la mission.

II - Préparation de la mission : examen de l'activité et élaboration d'un référentiel de risques



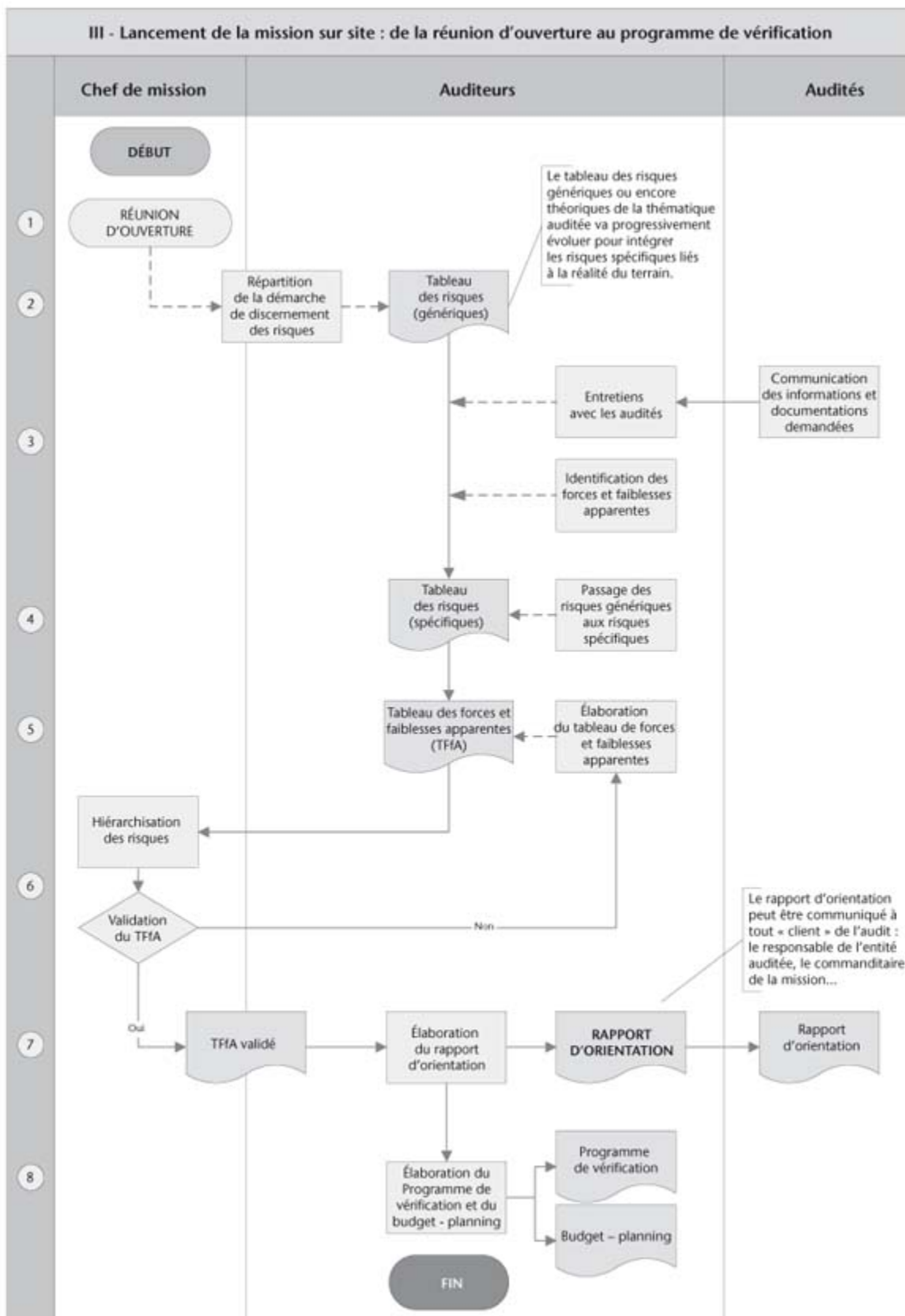
II - Préparation de la mission : examen de l'activité et élaboration d'un tableau des risques

Tâches réalisées / responsables concernés Modalités d'Application (MA) & Techniques d'Audit (TA) & Documents associés (DA)

Voir MA : l'examen de l'activité et son découpage en objets auditables

Voir MA : l'élaboration d'un tableau des risques

- 1 – Les auditeurs doivent en premier lieu étudier les documents récupérés auprès des responsables audités et les synthétiser afin de cerner le contexte de la mission et l'évolution du domaine d'activité auditée. En synthèse l'auditeur doit maîtriser 3 dimensions :
 - Les volumes et types de transactions (TA : volume et type de transaction) :
 - * Quels sont les enjeux de l'organisation ? objectifs stratégiques, opportunités globales ...
 - * Quelle est l'importance de l'organisation ? nombre salariés, CA, volume des transactions, place dans le groupe...
 - * Comment est elle structurée ? structure hiérarchique / matricielle...
 - * Y a-t-il des liens de dépendances entre une partie de l'activité et une autre ? si oui de quel type et de quelle importance ?
 - L'analyse économique et financière (TA : analyse économique et financière) :
 - * Repérer les activités concernées : divisions, produits, clients...
 - * Chiffrer les activités.
 - * Classer les activités par ordre d'importance.
 - * Comparer les indicateurs d'exploitation à différentes périodes et noter les évolutions.
 - * Comparer ces résultats avec les objectifs de l'organisation : y a-t-il des écarts ? sont ils importants ? où y en a-t-il le plus ? quelles seraient leurs causes (mauvaise définition des objectifs, des responsabilités...) ?
 - * Repérer les évolutions négatives et tenter de les expliquer (conjoncture, restructuration dans le cadre d'une stratégie groupe...).
 - L'examen d'activité ou comment fonctionne l'activité en général ?
 - * Quels sont les objectifs de l'activité, y compris leur cohérence avec les politiques et la stratégie de l'organisation ?
 - * Comment est organisée l'activité (organigramme) ? qui est responsable de quoi (niveaux d'intervention) ?
 - * Quels sont les moyens dont dispose chaque responsable pour atteindre les objectifs (moyens humains, financiers, matériels, systèmes d'informations) ?
 - * Quelles sont les méthodes de travail de l'organisation (procédures, instructions, lois...) ?
 - * Comment se répartit l'activité (cartographie des processus, répartition des opérations par poste) ?
 - * Quels sont les résultats et le dispositif de suivi ?
- 2 – À ce stade, soit le service d'audit interne dispose d'une bibliothèque de référentiels de risques préétablis, soit il s'agit d'une nouvelle thématique qui nécessite la conception d'un référentiel nouveau. L'existence de référentiels préétablis s'explique lorsque la fréquence et la récurrence de la thématique auditée justifie l'investissement « temps » consacré à son élaboration.
- 3 – En fonction des cas :
 - * Si le référentiel existe, les auditeurs s'assurent qu'il correspond bien à la problématique de la mission et l'adaptent éventuellement.
 - * Si le référentiel est à créer : il s'agit de découper la thématique auditée en domaines et/ou sous-domaines (MA : l'examen de l'activité et son découpage en objets auditables) et de se livrer ensuite à une démarche d'analyse de risques pour chacune de ces parties (MA : l'élaboration d'un tableau des risques).
- 4 – L'équipe d'audit dispose d'un tableau des risques (DA : tableau des risques) qui va servir de guide tout au long du déroulement de la mission. Il décompose la thématique auditée en domaines et/ou sous-domaines et, pour chacune de ces parties, il présente : les finalités de contrôle interne, les risques (scénarios d'empêchement, points de contrôle et impacts) et les bonnes pratiques de contrôle interne. Il va servir de base de référence par rapport à laquelle l'équipe d'audit va apprécier la réalité du terrain.
- 5 – Ce référentiel ainsi établi va ensuite successivement faire l'objet de plusieurs validations :
 - * Une pré-validation par le chef de mission qui s'assure que le référentiel couvre bien toutes les problématiques de la thématique auditée et notamment celles évoquées dans l'ordre de mission.
 - * Une présentation éventuelle aux audités pour qu'ils valident la base de référence par rapport à laquelle va se dérouler la mission d'audit. Si certaines préoccupations des audités en matière de risque n'ont pas été intégrées, des ajustements sont apportés par les auditeurs afin de répondre au mieux aux attentes des audités.
 - * Une validation définitive du référentiel par le chef de mission.
- 6 – Le tableau des risques validé peut faire l'objet d'une saisie dans un logiciel d'audit afin de faciliter et d'optimiser la réalisation des étapes ultérieures de la mission d'audit.



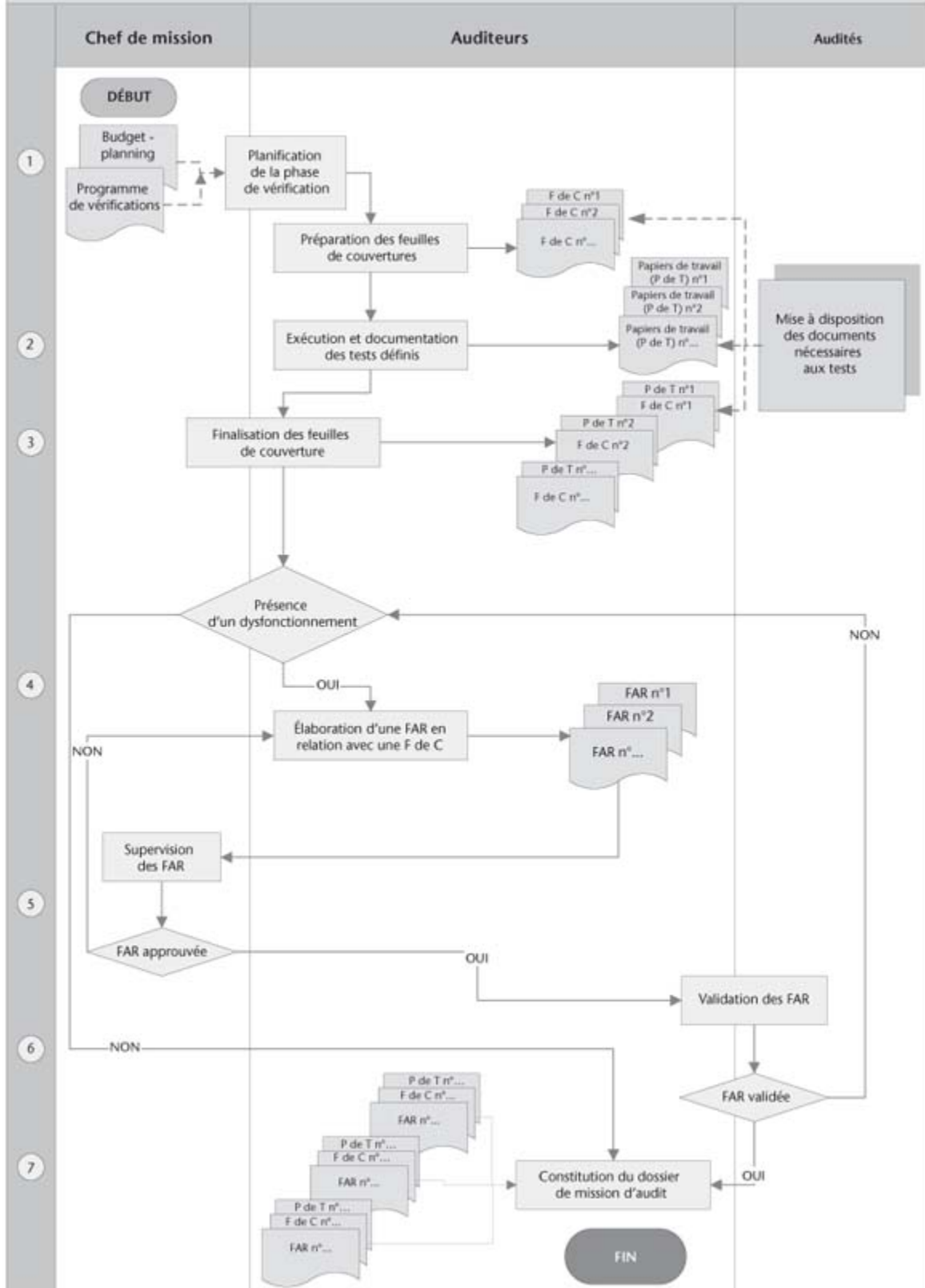
III - Lancement de la mission sur site : de la réunion d'ouverture au programme de vérification

Tâches réalisées / responsables concernés Modalités d'Application (MA) & Techniques d'Audit (TA) & Documents Associés (DA)

Voir : MA - la réunion d'ouverture, MA - l'analyse des forces et faiblesses
MA - le rapport d'orientation, MA - le programme de vérification

- 1 – Le chef de mission a pour objectif d'assurer le pilotage de la mission d'audit, de l'installation de l'équipe (réunion d'ouverture) (MA : la réunion d'ouverture) jusqu'à la restitution du rapport. À ce titre il est le représentant de l'équipe d'audit auprès des audités et du demandeur. Il prend donc en charge :
 - 1 - La veille au respect du périmètre de la mission défini dans l'ordre de mission.
 - 2 - L'organisation de la réunion d'ouverture. La réunion doit aborder 5 points clés :
 - * Présentation de l'équipe aux responsables audités.
 - * Présenter le but et la politique du service d'audit interne.
 - * Expliquer les raisons et les circonstances de la mission.
 - * Exposer la chronologie des aspects abordés (incluse le planning des entretiens).
 - * Mettre en place la logistique nécessaire à la conduite de la mission (bureau, téléphone...).
- 2 – Le chef de mission répartit en fonction des compétences et de l'expérience de chaque auditeur composant l'équipe la démarche de discernement des risques en s'appuyant sur le tableau des risques préalablement établi (domaines et sous-domaines auditables).
- 3 – L'équipe d'audit mène sous la supervision du chef de mission des interviews (TA : interviews) auprès du directeur des audités et des responsables audités afin de discerner les risques inhérents à l'organisation et à la mission. Dans le cadre de cette démarche, les auditeurs peuvent synthétiser les informations au moyen de diverses techniques : diagramme de circulation des flux (TA : diagramme de circulation), grilles des incompatibilités de tâches (TA : grille de séparation des tâches)... Le tableau des risques génériques sert de fil conducteur aux problématiques de risques abordées durant les différents entretiens. Il permet aux auditeurs d'être exhaustif dans leur approche de détection des risques spécifiques de l'entité auditée.
Les données collectées à cet effet permettent d'identifier les risques apparents.
Les audités apportent leur collaboration aux auditeurs lors des interviews. Ils leur communiquent tous les documents et informations nécessaires à l'identification des forces et faiblesses apparentes de l'organisation.
- 4 – L'équipe d'audit effectue les modifications nécessaires au tableau des risques (qui référence les risques génériques) en vue d'élaborer le tableau de forces et faiblesses apparentes (qui référence les risques spécifiques).
Dans le cas où un risque n'aurait pas été préalablement recensé ou qu'un risque n'est finalement pas présent, les auditeurs peuvent ajouter ou supprimer des rubriques au tableau d'origine.
- 5 – L'élaboration du tableau des forces et faiblesses apparentes (MA : l'analyse des forces et faiblesses) consiste en la mise en parallèle des forces et faiblesses recensées dans l'organisation avec les finalités de contrôle interne recensées précédemment au niveau du tableau des risques génériques. Ce tableau permet à l'équipe d'audit d'organiser la suite de la mission notamment au niveau du programme de vérifications.
- 6 – La hiérarchisation des risques et donc des objectifs de la mission est faite en fonction du découpage en objet auditables fait lors de l'élaboration du tableau des risques, et des forces et faiblesses relevées lors de la démarche de discernement des risques. Le chef de mission peut hiérarchiser les risques suivant plusieurs critères :
 - * L'importance financière estimée de leur conséquences (impact des risques).
 - * Leur probabilité d'occurrence.
 - * Leur capacité à influencer sur l'atteinte des objectifs.
 - * La facilité à mettre en place les bonnes pratiques.
 En final le chef de mission valide le tableau de forces et faiblesses apparentes.
- 7 – Une fois le tableau des forces et faiblesses apparentes validé, le chef de mission établit le rapport d'orientation (MA : le rapport d'orientation). Le rapport d'orientation (DA : rapport d'orientation) constitue une synthèse à mi-parcours de la mission d'audit, il récapitule les objectifs hiérarchisés que se fixe l'équipe d'audit dans le cadre de sa mission. Ces objectifs seront reflétés dans le programme de vérification. Ce document peut être communiqué à tout client de l'audit (responsable de l'entité auditée, commanditaire de la mission...).
- 8 – En final l'équipe d'audit établit les différents documents qui vont permettre de structurer et planifier la phase suivante de vérification. Ces documents sont établis en cohérence avec les objectifs de la mission présentés dans le rapport d'orientation, il s'agit :
 - * Du programme de vérification (MA : le programme de vérification et DA : programme de vérifications) qui précise le nombre et la nature des contrôles et tests à réaliser, ainsi que la répartition des travaux de contrôle entre les membres de l'équipe d'audit.
 - * Du « budget - planning » (DA : budget planning) qui permet de planifier les opérations de contrôle et de faciliter, par la suite, le suivi des temps alloués à chaque auditeur.
 À ce stade, l'équipe d'audit dispose de toutes les informations nécessaires à la poursuite de sa mission (hiérarchisation des objectifs de la mission, nature des travaux à réaliser, planification des opérations, outil de suivi des temps).

IV - Conduite des vérifications, de la feuille de couverture à la FAR



IV - Conduite des vérifications, de la feuille de couverture à la FAR

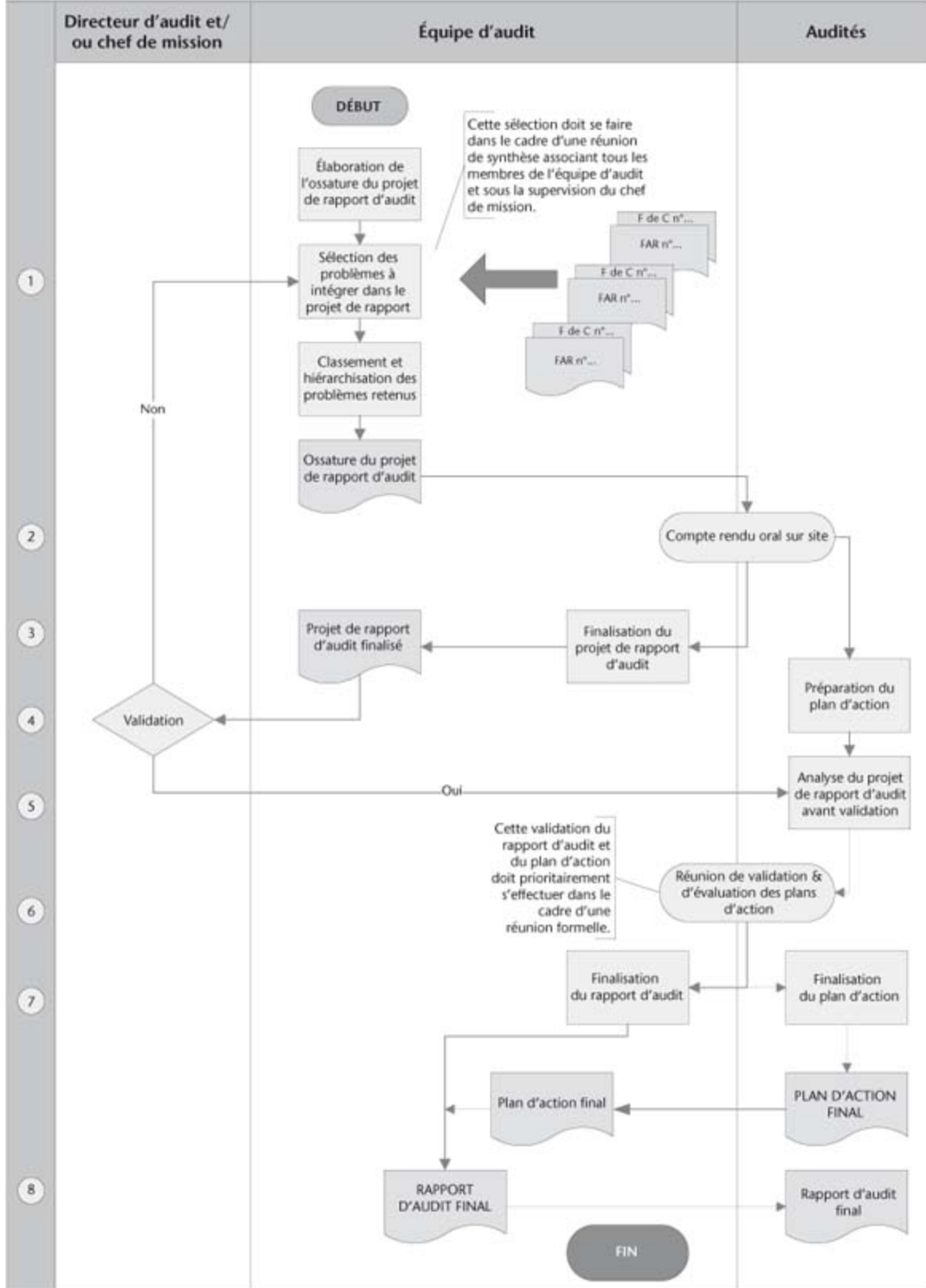
Tâches réalisées / responsables concernés
Modalités d'Application (MA) & Techniques d'Audit (TA) & Documents Associés (DA)

MA : La formalisation des travaux de contrôle (papier de travail et feuille de couverture)

MA : La fiche d'audit et de recommandations

- 1 – Le chef de mission est responsable de l'édition et de la communication du programme de vérifications (**DA : programme de vérifications et budget – planning**) qui répartit l'ensemble des travaux à effectuer pour chaque objectif du rapport d'orientation entre les auditeurs. Tout au long de la mission, le chef de mission devra s'assurer du suivi effectif du programme de vérifications et superviser la qualité des travaux effectués. La réalisation des tests et contrôles est donc répartie entre les membres de l'équipe d'audit et planifiée sur la durée de cette phase de vérification.
- 2 – Les auditeurs réceptionnent le programme de vérification et initialisent les feuilles de couverture (**DA : feuille de couverture**) en fonction des tâches référencées dans celui-ci.
Chaque tâche est affiliée à un objectif du rapport d'orientation et fait l'objet d'une ou plusieurs feuilles de couverture qui donneront lieu à un ensemble de vérifications définies lors de l'initialisation des feuilles de couverture.
La réalisation des vérifications auprès des audités se fait suivant différentes techniques d'audit : des interviews (**TA : interviews**), des sondages (**TA : sondages statistiques**), de tests de cheminement (**TA : piste d'audit**), des constatations (**TA : observations physiques**), des rapprochements de documents (**TA : rapprochement et reconstitutions**), des contrôles informatiques (**TA : interrogations des fichiers informatiques**). Le détail des travaux réalisés est formalisé par les auditeurs sur des papiers de travail (**MA : la formalisation des travaux de contrôle**) qui constitueront les preuves qui étayeront les conclusions de l'audit et servent à finaliser les feuilles de couverture.
Les audités s'assurent que les auditeurs disposent de tous les documents leurs permettant de mettre en application le programme de vérification et collaborent à la démarche d'audit.
- 3 – Le chef de mission participe à la finalisation de toutes les feuilles de couverture (**MA : la formalisation des travaux de contrôle**), mais il peut aussi participer à leur élaboration si le programme de vérification est défini en ce sens. La finalisation d'une feuille de couverture consiste à relater, au regard des objectifs du test, les résultats obtenus et l'opinion de l'équipe d'audit quant à un dysfonctionnement avéré ou non. Ces résultats constitueront les éléments de **preuve** des dysfonctionnements relatés ultérieurement.
- 4 – Lorsque toutes les feuilles de couverture prévues sont établies, l'équipe d'audit conclut sur la présence ou non d'une faiblesse de contrôle interne de l'organisation auditée.
Les feuilles de couverture où aucun dysfonctionnement n'est décelé par l'équipe sont archivées directement dans le dossier d'audit. Les feuilles de couverture qui attestent d'un dysfonctionnement donneront lieu à la formalisation d'une feuille d'audit et de recommandations (**MA : la fiche d'audit et de recommandations**) (**DA : fiche d'audit et de recommandations**). Chaque FAR est rédigée par l'équipe d'audit.
Une FAR permet de caractériser le dysfonctionnement par :
 - * Des faits constatés servant de preuves (pas de jugement ou de supposition).
 - * Des causes logiques ou historiques (pas de constat ponctuel).
 - * Des conséquences mesurées ou estimées (risques avérés ou potentiels).
 - * Un problème synthétisant de façon complète et percutante le dysfonctionnement.
 - * Une recommandation (ou plus précisément une proposition de recommandation).
- 5 – Une fois les FAR établies, le chef de mission exerce son rôle de supervision. L'approbation d'une FAR se fait en fonction :
 - * Du dysfonctionnement en lui-même : Est-il si grave ?
 - * Des preuves attestant du dysfonctionnement : Sont-elles suffisantes ?
 - * De la formulation du problème : Est-elle synthétique, complète et facile à mémoriser ?
 - * De la qualité des recommandations : Sont-elles « vendables » (applicables, opportunes...) ?
- 6 – Les audités peuvent être amenés à valider les feuilles d'audit et de recommandations qui leur sont présentées par les auditeurs. Ils prennent connaissance du problème, s'en informent et peuvent ainsi y répondre ou en préparer les recommandations en collaboration avec l'auditeur rédacteur de la FAR. La validation de l'audité lui permet de prendre connaissance et d'apprécier un dysfonctionnement mais pas de remettre en cause son existence dans la mesure où les éléments de preuve sont suffisamment probants.
Dans le cas d'un désaccord entre l'auditeur et l'audité sur le contenu d'une FAR, celle-ci sera revue autant de fois que nécessaire, mais en aucun cas l'audité ne pourra exiger la suppression de la FAR sans l'accord du chef de mission.
- 7 – Le chef de mission, centralise tous les papiers de travail (P de T), les feuilles de couverture (F de C), ainsi que les fiches d'audit et de recommandations (FAR) afin de constituer le dossier d'audit à la disposition de chaque auditeur. La centralisation de ces documents permet au chef de mission de procéder à leur référencement selon la codification retenue. Le dossier d'audit qui structure et conserve tous les éléments établis durant la mission regroupe tout le savoir faire « audit » mis en oeuvre durant la mission. Il pourra servir lors de missions d'audit ultérieures de même nature.
Le dossier d'audit décrit et évalue en détail le travail effectué afin de permettre à chaque auditeur d'avoir une vue d'ensemble de la mission et donc de permettre les rapprochements entre papier de travail, feuille de couverture et fiche d'audit et de recommandations associées.
En parallèle de l'établissement du dossier d'audit, le chef de mission prend en charge l'établissement du dossier administratif où sont référencés de manière synthétique l'état d'avancement de la mission, les objectifs ou tâches en suspens, les notes de frais ainsi que les correspondances entre l'équipe et le demandeur. Le dossier administratif constitue une annexe du dossier d'audit.

V - Rédaction des conclusions : de l'ossature du rapport d'audit à sa validation



V - Rédaction des conclusions : de l'ossature du rapport d'audit à sa validation

Tâches réalisées / responsables concernés

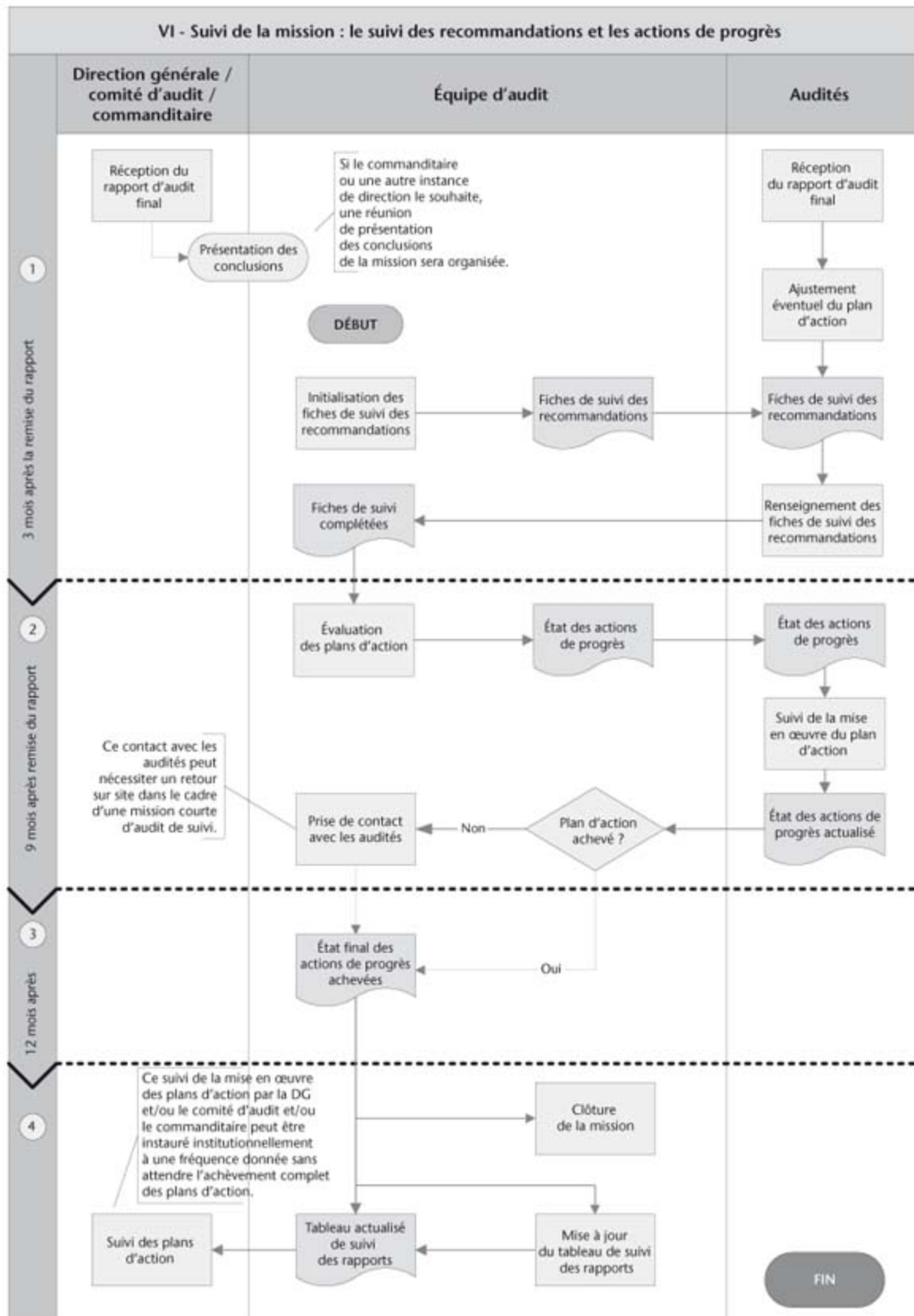
Modalités d'Application (MA) & Techniques d'Audit (TA) & Documents Associés (DA)

MA : l'ossature du rapport

MA : le compte rendu final sur site

MA : le rapport d'audit et sa validation

- 1 – La réunion de synthèse doit récapituler l'ensemble des problèmes référencés dans les fiches d'audit et de recommandations (FAR) afin de les classer par division, thème ou processus, puis les hiérarchiser. Sont aussi abordés durant la réunion les éventuels supports de présentation qui seront utilisés auprès des audités ainsi que l'orientation générale du rapport (sélection des FAR). Lors de cette réunion, le travail des auditeurs sur les dysfonctionnements est synthétisé, remis en forme, afin que les problèmes soient classés et hiérarchisés en fonction des résultats des tests. L'équipe d'audit établit l'ossature du rapport d'audit (MA : l'ossature du rapport) afin de faciliter la communication avec les audités lors du compte rendu final sur site.
- 2 – Avant la rédaction du rapport projet, l'équipe d'audit effectue un compte rendu oral (MA : le compte rendu oral sur site) auprès des principaux responsables audités où ces derniers sont informés des problèmes sélectionnés lors de la réunion de synthèse, de l'importance de ces problèmes et de la date de la réunion de validation. Ce compte rendu oral donne aux audités la possibilité de se préparer à la lecture du projet de rapport. Les audités sont informés lors d'un compte rendu oral du déroulement global de la fin de mission par l'équipe d'audit ainsi que des principaux problèmes qui ont été relevés lors de la mission et de leur importance. Cela leur permet par la suite de débiter la réflexion au sujet d'un plan d'action suite à l'audit.
- 3 – Suite au compte rendu oral sur site, l'équipe d'audit établit sur la base de l'ossature du rapport le projet de rapport d'audit (DA : projet de rapport d'audit) en intégrant les remarques des audités (MA : le rapport d'audit et sa validation).
- 4 – Le projet de rapport d'audit est présenté au responsable de l'audit interne, afin d'être validé :
 - * Les problèmes énoncés sont-ils dans le champ de la mission ?
 - * Les résultats des tests effectués sont-ils probants au regard des dysfonctionnements identifiés ?
 - * Les recommandations sont-elles pertinentes (adaptées aux problèmes à résoudre) ?
 Ce n'est que si le projet de rapport d'audit est validé que ce dernier pourra être présenté aux audités en préparation de la réunion de validation.
 Si le projet de rapport d'audit n'est pas validé, l'équipe d'audit reconsidère ses conclusions.
- 5 – Le projet de rapport d'audit validé par la direction de l'audit est communiqué aux audités avant la réunion de validation afin qu'ils puissent être informés des conclusions formalisées de la mission d'audit et ainsi préparer efficacement la réunion de validation en complétant éventuellement leur plan d'action.
- 6 – La validation du projet de rapport est faite dans le cadre d'une réunion de validation avec les audités (MA : le rapport d'audit et sa validation). Durant cette réunion, l'équipe d'audit présente les conclusions de sa mission. Le directeur de l'entité auditée peut, dans le cadre de cette réunion, se faire assister de ses principaux collaborateurs.
 Au terme de la réunion, l'équipe d'audit devra :
 - * Valider le corps du rapport FAR par FAR : les solutions proposées conviennent-elles aux problèmes évoqués ?
 - * Avoir désigné un responsable audité pour la mise en œuvre de chaque recommandation. La désignation des responsables qui devront piloter la mise en œuvre des recommandations est à la charge des audités.
 - * Avoir obtenu une ébauche de plan d'action. Le plan d'action est initié par les audités en collaboration avec l'équipe d'audit lors de cette réunion.
 Dans le cas d'un désaccord persistant avec les audités sur le fond du projet de rapport ou la présence d'une FAR, l'équipe d'audit devra mentionner en annexe le point de vue des audités concernant le problème visé.
- 7 – Suite à la réunion de validation, les audités finalisent le plan d'action et le communique à l'équipe d'audit qui l'intègre au rapport final. Parallèlement, les auditeurs rédigent le rapport d'audit final. Il s'agit de compléter le projet de rapport par :
 - * Une synthèse qui comprend en introduction les remerciements de l'équipe d'audit et les spécificités du rapport d'audit. La synthèse reprend l'opinion générale de l'équipe d'audit sur le fonctionnement global de l'organisation auditée, les points forts ainsi que les principaux dysfonctionnements répertoriés durant la mission.
 - * Une partie rédactionnelle détaillée plus particulièrement destinée aux audités.
 - * Le plan d'action défini par les audités.
 - * Des annexes éventuelles.
 Par ailleurs, une note de synthèse destinée à la direction générale peut être établie séparément si nécessaire.
- 8 – Le rapport d'audit final ainsi établi est communiqué aux audités (responsable de l'entité auditée et/ou ses collaborateurs), au commanditaire de la mission et aux destinataires institutionnels des rapports d'audit (direction générale, direction financière, directions fonctionnelles concernées...). Cette opération clôture la mission d'audit pour l'équipe d'auditeurs concernés. Ils peuvent donc être affectés à une nouvelle mission. Cependant le service d'audit interne (les auditeurs ayant réalisés la mission, d'autres auditeurs du service ou une équipe dédiée) doivent s'assurer de la mise en œuvre des plans d'action.



VI - Suivi de la mission : le suivi des recommandations et les actions de progrès

Tâches réalisées / responsables concernés Modalités d'Application (MA) & Techniques d'Audit (TA) & Documents associés (DA)

MA : le suivi des recommandations MA : l'état des actions de progrès

- 1 – DURANT LES 3 MOIS SUIVANT LA REMISE DU RAPPORT D'AUDIT (MA : le suivi des recommandations) :
 - * Les audités ajustent éventuellement le plan d'action au regard du rapport d'audit reçu afin d'obtenir un plan d'action définitif.
 - * La mise en œuvre des recommandations est effectuée dès que le plan d'action est définitif et peut s'étaler sur les 9 mois suivants.
 - * L'équipe d'audit fait parvenir aux audités les fiches de suivi des recommandations pré-établies associées à chaque recommandation (DA : fiche de suivi des recommandations).
 - * Les audités doivent compléter les fiches de suivi des recommandations dans les 3 mois suivant leur réception en associant une partie du plan d'action (résumée si nécessaire) à une recommandation. Ils devront aussi mentionner sur la fiche de suivi :
 - . La décision concernant la recommandation énoncée. Si celle-ci n'est pas retenue, le responsable audité ayant avalisé le refus devra en énoncer la raison.
 - . Le responsable de la mise en œuvre de la recommandation.
 - . L'échéance de mise en œuvre de la recommandation.
 - . La date de report et l'objectif de la réflexion concernant la recommandation si celle-ci est mise à l'étude.
 - * L'équipe d'audit récupère les fiches de suivi des recommandations complétées par les audités durant les 3 mois suivant la remise du rapport.
- 2 – DANS LES 9 MOIS SUIVANT LA REMISE DU RAPPORT D'AUDIT (MA : l'état des actions de progrès) :
 - * Une première évaluation sur la mise en application et l'acceptation des recommandations est effectuée lors de la réception des fiches de suivi. Dans cette évaluation, l'audit interne s'assure que le problème lié à la mission est traité : il ne s'agit pas d'évaluer le fonctionnement global de l'organisation dans la mise en place des recommandations ou de participer à la mise en place des recommandations. Ce bilan, formalisé dans l'état des actions de progrès (DA : état des actions de progrès EAP), est renvoyé aux audités en vue du suivi effectif de la mise en œuvre du plan d'action dans sa totalité.
 - * Si toutes les recommandations retenues ont été mises en œuvre, la transmission aux audités d'un EAP actualisé (bilan de la mise en place des recommandations à 3 mois puis à 9 mois), aboutit à la clôture définitive de la mission d'audit.
- 3 – DANS LES 12 MOIS SUIVANT LA REMISE DU RAPPORT D'AUDIT (MA : l'état des actions de progrès) :
 - * Si certaines recommandations retenues par les audités n'ont pas été mises en œuvre, l'équipe d'audit prend contact avec les audités, dans le cadre éventuellement d'une réunion ou d'un retour sur site si nécessaire, afin d'en apprécier les raisons.
 - * L'équipe d'audit met définitivement à jour l'état des actions de progrès et clôture la mission d'audit.
- 4 – EN FINAL :
 - * L'équipe d'audit met à jour le tableau de suivi des rapports (synthèse des états des actions de progrès des différentes missions réalisées).
 - * Ces informations sont transmises au commanditaire, à la direction générale, au comité d'audit pour information et prise de décision éventuelle en cas de retard dans le planning de mise en œuvre des recommandations.

L'Essentiel

- L'objet d'une mission d'audit interne est d'étudier la maîtrise des risques de l'activité, le processus ou l'entité qu'on audite – étude au sens large : analyse, examen, identification des lacunes, élaboration de solutions (avec les audités), suivi de la mise en oeuvre des plans d'action des audités ; en bref, ce que fait le médecin généraliste avec son patient lorsqu'il effectue son diagnostic, réalise son pronostic et préconise sa thérapeutique.
- Les six processus de conduite d'une mission sont : l'initialisation de la mission, la préparation de la mission, le lancement de la mission sur site, la conduite des vérifications, la rédaction des conclusions et enfin le suivi de la mission.
- Du fait de l'architecture de la présentation de cette partie « Méthodologie de l'audit », le lecteur pourra en fonction de sa connaissance du métier :
 - soit se contenter des schémas et pages de commentaires associées ;
 - soit approfondir certains processus en prenant connaissance des chapitres 6 « Modalités d'application » et/ou 8 « Techniques d'audit ».
- Une mission d'audit opérationnel peut durer de quelques jours à quelques mois, selon l'envergure du sujet et le nombre d'auditeurs. Le plus fréquent est de quatre à dix semaines pour une mission nouvelle avec deux à quatre auditeurs dont un chef de mission.

Chapitre 6

Les modalités d'application (MA)

EXECUTIVE SUMMARY

- Quels sont les étapes et produits méthodologiques à respecter pour mener à bien une mission d'audit interne ?
- Quels sont les trucs et astuces pour bien réussir sa mission d'audit en regard des retours d'expériences professionnelles observés ?
- Les modalités d'application (MA) présentées dans les six processus du chapitre 5 sont reprises ci-après d'une manière structurée et complétées par des « fiches pratiques » et des « focus ».

LE DROIT D'ACCÈS : LA LETTRE OU L'ORDRE DE MISSION

Pour rechercher les risques, les prouver et les démontrer, etc., il faut aller voir ! L'auditeur doit accéder à l'information qui remonte (comptabilité, reporting, risques, compliance...) et aux locaux et installations, équipements, registres, documents et personnes concernées. C'est évident mais l'auditeur a-t-il un droit d'accès illimité ? L'auditeur a plein accès quand et seulement quand il est mandaté ; après la mission il n'a plus cet accès. Donc toute mission d'audit commence par un mandat.

Comment cela se présente-t-il ? Il faut un document qui fasse comprendre à ses destinataires sur quoi porte le droit d'accès des auditeurs et leur devoir de communication aux auditeurs, en gros le périmètre de la mission – en terme technique on dit le « champ » de la mission ou si l'on parle franglais, son « scope ». Il est habituel d'indiquer aussi la raison d'être de cette mission – on dit parfois ses « objectifs », mais à ce stade ils sont brefs et peu détaillés. Dans certaines organisations, cela se fait en communiquant le plan d'audit (ou une partie du plan d'audit), le plus souvent en émettant un ordre ou une lettre de mission comme ci-dessous.

Direction : Générale Service : Audit interne	Date : 5 janvier 2020 Réf. : PSK 03/58
Objet : Audit des achats usine HA	
<p>Conformément aux décisions du comité d'audit du 16 décembre 2019, le service d'audit interne commence, à la demande de la direction de la branche, un audit des achats de l'usine HA.</p> <p>Les objectifs généraux sont les suivants :</p> <ul style="list-style-type: none"> – apprécier l'organisation en vigueur et les systèmes d'informations existants ; – s'assurer de l'efficacité des procédures mises en œuvre pour prévoir, effectuer et suivre les achats (commandes, réceptions, règlements) ; – évaluer les gains réellement apportés par le système GAPACHA récemment mis en place. <p>Cette mission commencera le 15 janvier 2020 et s'étendra sur environ six semaines. Elle sera menée par Ch. Demisse (téléphone : ...) assisté de A. Tricin et A. Teurdeux.</p> <p>Vous voudrez bien en informer les personnes concernées et prêter votre concours actif au bon déroulement de cette mission.</p>	
X	pour la direction générale C. Padlablag
Destinataires : Le directeur de la branche Jean Veux, D. Uzin, D. Fel Copie : membres du comité exécutif	

Commentaires sur cet ordre de mission :

- il est signé par la DG, c'est indispensable (quelquefois directement signé par le directeur de l'audit, s'il s'appuie sur une décision de la DG) ;
- il ne comporte pas de date de fin : c'est regrettable car c'est peut-être ce qui intéresse le plus les audités... mais c'est prudent sauf forte contrainte organisationnelle ! ;
- ses destinataires sont le directeur de la branche, le chef des audités (directeur de l'usine), qui est supposé retransmettre à ses collaborateurs concernés, et le responsable fonctionnel (direction des achats de la branche) ;

- il a été rédigé par l'audit pour avoir les caractéristiques de forme et de fond souhaitées (éviter « Suite à de nombreuses erreurs et irrégularités, j'ai décidé... » ou « Les auditeurs me rendront personnellement compte des dysfonctionnements qu'ils auront découverts »).

Il est souhaitable de se concerter au préalable avec l'unité afin d'éviter les problèmes pratiques particuliers : déménagement dans le site ou réfection des peintures (donc dossiers inaccessibles), solde de congés des principaux interlocuteurs (par exemple les comptables après la clôture), annonce d'une restructuration et/ou début d'une grève, visite d'une mission d'étude étrangère ou du Président de la République...

Attention : le plan d'audit et sa documentation devraient permettre de rédiger immédiatement l'ordre de mission, mais parfois tout un travail préalable peut être nécessaire pour en dégager les contours (champ) et les axes (objectifs).

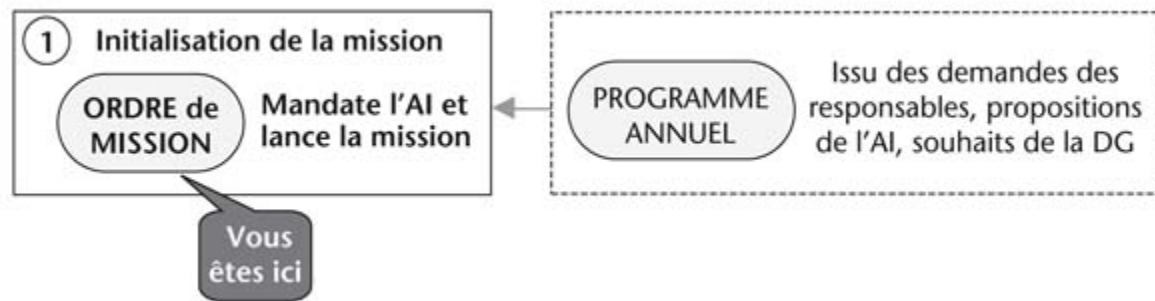
Par exemple, une direction rencontre des difficultés avec divers services de l'entreprise et la DG accepte de lancer une mission non planifiée. Il faut d'abord cerner de quoi il s'agit, et pour cela interviewer la direction demanderesse et les services, percevoir les problèmes, retenir ceux qui forment un tout cohérent (car chaque responsable vous parle de ses problèmes) et proposer un champ de mission et ses objectifs.

Ou bien on vous demande d'auditer le recrutement. S'agit-il du service recrutement et de son fonctionnement ? Ou du processus de recrutement, impliquant ce service, ses « clients » (les services demandant du personnel) et l'organisation de leurs relations ? Ou de la fonction recrutement : en plus du processus ainsi défini, comment met-on en œuvre les politiques et stratégies décidées (évolution du portefeuille de compétences, équilibre entre recrutement et promotion interne...) ?

En même temps, on va recueillir une première idée sur la chose à auditer : importance et organisation, finalités, objectifs, performances, frontières... Cela par lectures, rassemblement d'une documentation, interviews des directions hiérarchiques et fonctionnelles (notamment

contrôle de gestion, toujours bien informé), discussions avec des experts et sachants...

On va commencer à prendre conscience de ses risques habituels et de ses bonnes pratiques classiques pour les maîtriser, on va commencer l'élaboration du référentiel, on va vraiment démarrer la mission !



Focus

L'ordre de mission (OM) est le mandat donné par la direction générale à l'audit interne pour informer les responsables concernés de l'intervention imminente des auditeurs et donner le droit d'accès.

Retour d'expérience

Ce produit méthodologique est largement déployé par les entreprises, fréquemment signé par la direction de l'entreprise, quelquefois directement par l'audit interne notamment dans le cadre d'un plan d'audit annuel, rarement cosigné par le directeur de la structure auditée. Considéré comme un mandat, il est généralement envoyé avant l'intervention de l'audit, cependant certains services préfèrent attendre de disposer d'informations suffisantes sur le périmètre d'audit avant de rédiger l'ordre de mission, ce qui peut donner le sentiment de commencer à investiguer sans légitimité pour le faire.

L'EXAMEN DE L'ACTIVITÉ ET SON DÉCOUPAGE EN « OBJETS AUDITABLES »

Cette phase de préparation de la mission consiste à préciser le champ de l'audit, identifier les personnes à rencontrer, collecter la documentation sur les disciplines à auditer et sur les techniques d'audit existantes, obtenir des informations chiffrées ou caractéristiques du domaine audité. Les différentes directions contactées s'efforcent de faciliter ce travail de préparation indispensable.

Les auditeurs internes étudient toutes les informations utiles collectées concernant la société ou les activités à auditer, développent des questionnaires et mènent quelques interviews auprès des principaux responsables identifiés. Ces travaux vont permettre de constituer un référentiel du domaine à auditer, mener une analyse de risques et identifier des objectifs précis d'audit.

Pour une mission nouvelle, c'est le moment difficile : connaître et comprendre un domaine nouveau et préparer l'analyse de risques et ses « points de contrôle ». Mais, heureusement, c'est rare : la plupart des missions sont récurrentes, on peut partir de l'expérience acquise sur le même sujet dans une autre unité.

C'est le moment où l'expérience du sujet est une arme – connaissance de ses habituels risques et opportunités d'amélioration – mais une arme à double tranchant : il faut éviter de se piéger soi-même, de se focaliser sur les difficultés qu'on a personnellement rencontrées, en oubliant qu'il peut en exister d'autres (risques non avérés) ou que l'évolution des techniques et de l'organisation peut en avoir engendré de nouvelles (nouvelles méthodes et nouveaux risques).

La prise de connaissance du domaine à auditer est un travail classique : connaissance du sujet par des lectures diverses et connaissance de l'unité (ou des unités) à auditer : chiffres saillants, points marquants de l'histoire, organigrammes et définitions de fonctions, cartographie des risques...

Il y a lieu de lister tous les documents nécessaires à l'auditeur en vue de la prise de connaissance de l'entité auditée préalable à la mission. Lors de la phase d'étude, l'équipe d'audit doit :

- avoir une vision globale de l'organisation auditée ;
- identifier les processus où se situent les risques afin de ne pas étudier quelque chose hors de propos ;

- pouvoir estimer le temps et le coût des phases de la mission, et se donner une base pour élaborer le référentiel de l'activité auditée (tableau des risques) ;
- se donner une crédibilité en ayant une approche rigoureuse.

La phase de prise de connaissance du sujet peut être à durée très variable, cette durée variant en fonction de la complexité du sujet, du profil de l'auditeur et des documents dont dispose le service audit (dossiers et rapports d'audit précédents).

La prise de connaissance du sujet se regroupe en trois ensembles ayant chacun un thème précis :

- les volumes traités (voir TA : les volumes et types de transactions) ;
- l'environnement (voir TA : analyse économique et financière) ;
- l'organisation interne.

Ces informations peuvent être obtenues par des interviews menées par les auditeurs sur la base de questionnaires de prise de connaissance menés auprès du management de l'entité auditée.

Deux approches sont combinées : l'examen de l'activité et son découpage en objets auditables.

L'examen de l'activité

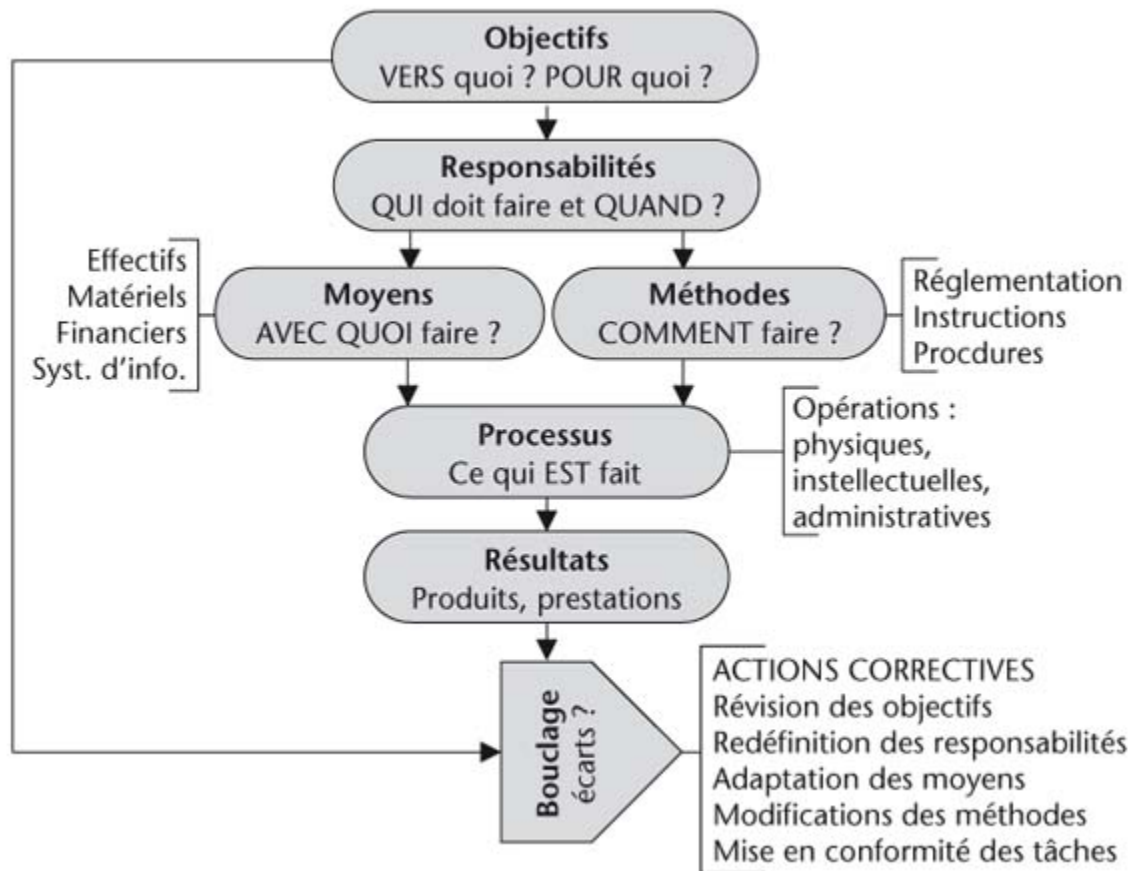
Le sujet à auditer, et/ou chacune de ses parties, doit être regardé du global au détaillé, du conceptuel au concret :

1. ses finalités et ses objectifs, y compris leur cohérence avec les politiques et la stratégie ;
2. les responsabilités ;
3. les moyens et méthodes ;
4. le processus, les tâches réalisées ou à réaliser ;
5. les résultats, leur suivi, et leur comparaison aux objectifs.

Utilisée dans un premier temps pour prendre connaissance du domaine à auditer, cette chronologie permet de comprendre et évite de se « noyer ». Appliquée dans un second temps à chaque stade du découpage, elle aide à dresser l'inventaire des objectifs et des risques.

L'examen d'activité permet à l'équipe d'audit de comprendre le fonctionnement opérationnel de l'organisation auditée. Afin d'en prendre connaissance de manière exhaustive, l'équipe d'audit devra chercher à obtenir les informations.

Figure 6.1 – Prise de connaissance du domaine audité. Examen d'une activité : schéma et progression.



EXEMPLES D'EXAMEN D'ACTIVITÉ

Objectifs et stratégie

- Quels sont les objectifs de l'organisation ? Sa politique pour les atteindre ? Dans quel but ?
- *Business plan*, guide de la politique de l'entreprise.
- Politique salariale.
- Politique clients/fournisseurs.
- Réformes prévues ou en cours.

Définition des responsabilités

- Comment est organisée l'activité ? Organigramme et structure.
- Qui est responsable de quoi ? Niveaux d'intervention, liste des délégations de pouvoir.
- Comment se répartit l'activité ? Cartographier les processus, repérer la répartition des opérations par poste.

Ressources (moyens)

- Quels sont les moyens dont dispose chaque responsable pour atteindre les objectifs ? Moyens humains, financiers, matériels.
- Comment sont répartis les moyens ? Par qui ?
- Structure de l'environnement informatique.

Pratiques de travail (méthodes)

- Quelle est la base de travail de l'organisation ? Base de pratique de travail, instructions, modes opératoires, lois, etc.
- Manuel de procédures internes et manuel qualité.
- Manuel de procédures générales.
- Juridique : informations réglementaires.
- Problèmes passés ou en cours.

Tâches – Processus

- Voir découpage du processus en objets auditables.

Résultats et suivi : reporting

- Analyser les tableaux de bord d'exploitation et les comparer dans le temps.
- Comparer ces résultats avec les objectifs de l'organisation : y a-t-il des écarts ? Sont-ils importants ? Où y en a-t-il le plus ? Quelles seraient leurs causes (mauvaise définition des objectifs, des responsabilités, etc.) ?

Le découpage en objets auditables

Il s'agit d'effectuer une décomposition du sujet de la mission en objets auditables afin de produire le référentiel d'audit.

Le processus à auditer sera découpé en éléments plus simples à appréhender, puis chacun étudié tour à tour, comme le recommande Descartes : « diviser chacune des difficultés... en autant de parcelles... qu'il serait requis pour les mieux résoudre ».

On découpe en **stades chronologiques** quand, cas le plus fréquent, la dimension chronologique est un guide. Par exemple, dans l'audit de la facturation, on aura probablement, entre autres : la sortie d'usine ou de magasin, le calcul et l'émission de la facture, la mise à jour de la comptabilité et des statistiques commerciales.

De même pour les achats, on aura les données suivantes.

EXEMPLE DE DÉCOUPAGE DU PROCESSUS « ACHATS » EN STADES D'ACTIVITÉS ET ÉTAPES CHRONOLOGIQUES = FINALITÉS EXEMPLES D'EXAMEN D'ACTIVITÉ

Objectifs/but/politique

Organisation/responsabilités

Moyens

Méthodes

Découpage du processus

1. Expression et justification du besoin
 2. Sélection du fournisseur
 3. Passation de la commande (du contrat) au fournisseur
 4. Réception de la marchandise (y compris entrée en stock) ou de la prestation
 5. Réception de la facture et comptabilisation de la facture
 6. Paiement de la facture et comptabilisation du paiement
- Autres étapes : traitement des litiges, refus de la marchandise et événements liés...

Pilotage/bouclage

Quand le découpage chronologique ne peut être utilisé, on découpe par **arborescence sémantique**. Par exemple, pour une facturation de flux continu (électricité, téléphone...) où les événements sont des changements d'options ou de tarifs une fois le contrat initial mis en route, on se dira :

- qu'est-ce que facturer ? C'est probablement : facturer toutes les prestations, aux conditions tarifaires en vigueur, et dans des délais brefs. On reprend chacun de ces points et on continue ;
- qu'est-ce que les conditions tarifaires en vigueur ? C'est probablement : les conditions de prix et les conditions de paiement. On reprend chacun de ces points et on continue ;
- qu'est-ce que les conditions de paiement ? C'est les délais de paiement et les moyens de paiement.

Nous sommes arrivés à la fin de l'arborescence, pour cette feuille de cette branchette de cette branche, car délais et moyens de paiement

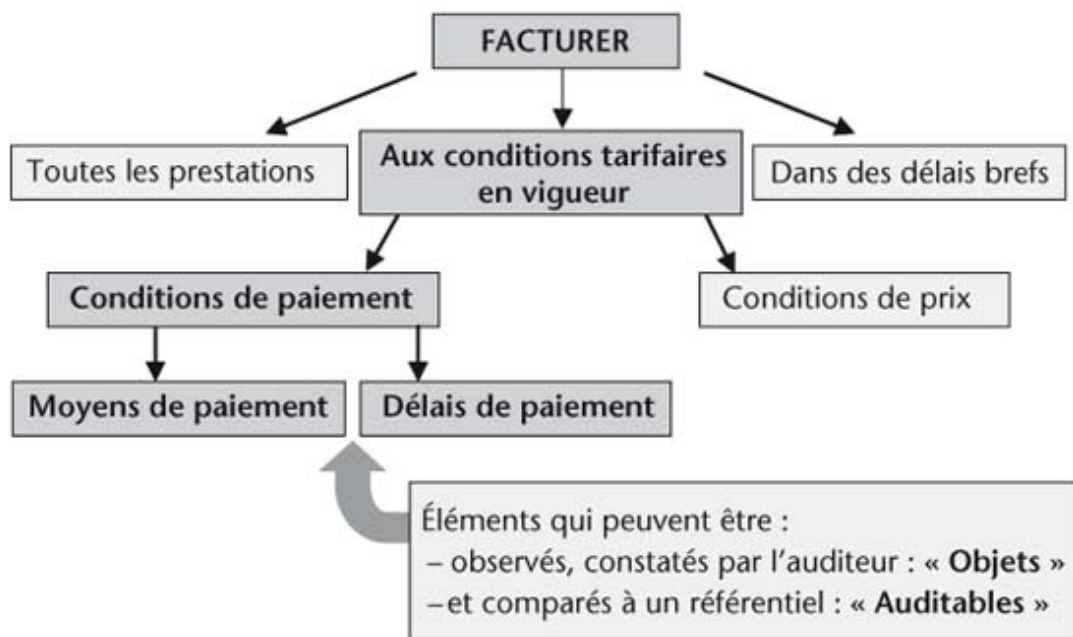
sont des choses concrètes, des « objets ».

En complément à cette approche, on pourra vérifier l'exhaustivité des préoccupations par l'approche qualité : quels sont les partenaires de la facturation, quelles sont leurs attentes ? Ici, nous avons oublié les clients (envoyer la facture au bon client), la comptabilité et les statistiques de vente, le recouvrement... !

On a maintenant terminé d'identifier les « objets auditables ». Chaque élément peut servir à élaborer le référentiel de l'activité, puis être observé, constaté et comparé par l'auditeur.

EXEMPLE DE DÉCOUPAGE PAR ARBORESCENCE

« Facturation suivant consommation » sans la séquence classique expédition – facturation (téléphonie, reprographie...)

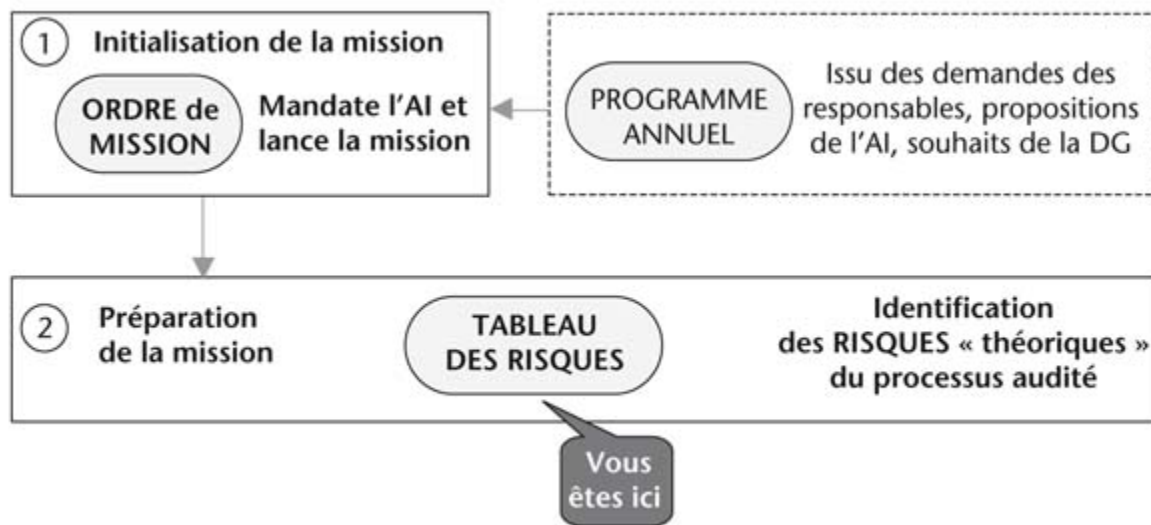


L'élaboration du référentiel d'audit consistera pour chacun des « objets », comme cité plus haut, à dresser l'inventaire des objectifs et des risques, puis pour chaque couple objectif/risques (risques au pluriel : il peut y avoir plusieurs risques de non-atteinte d'un objectif), de développer les modalités de fonctionnement qui garantissent l'atteinte de ces objectifs en évitant ces risques : les bonnes pratiques d'organisation communément adoptées. C'est bien évidemment ici que

l'expérience, une bonne documentation ou de bons conseillers sont les plus utiles !

La prise de conscience des habituels risques et opportunités d'amélioration est plus délicate (ne pas oublier le centre de documentation des institutions professionnelles... ni les collègues et anciens collègues qui ont peut-être déjà traité la question !).

RÉFÉRENTIEL D'AUDIT : L'ÉLABORATION D'UN TABLEAU DES RISQUES



Le tableau des risques (TaRi) constitue l'outil de référence qui permet à l'auditeur d'une part de définir le champ et les limites de ses investigations et d'autre part, de structurer la présentation de ses analyses et conclusions, notamment pour renseigner ce qui relève de constat(s), la ou les causes des faits constatés ainsi que leurs conséquences.

Lorsque l'audit porte sur des missions « classiques » du type dépenses ou recettes, achats – dépenses de personnel ou vente –, la matière permettant l'exercice de la construction d'un référentiel existe,

soit contenue dans des notes de politique interne soit dans des manuels de présentation de méthode de contrôle interne. Pour des missions nouvelles et à caractère particulier (objet de mission très large portant sur de l'organisationnel ou sur des aspects qualitatifs), l'établissement du TaRi demeure un exercice difficile. La question est, en général, par où vais-je commencer ? Quel est le point de départ de ma réflexion ?


Les concepts exposés ci-après doivent faciliter l'approche de la construction d'un TaRi.

Le tableau de risques proposé privilégie l'enrichissement de la colonne « Risques » = empêchements + points de contrôle + impacts par rapport à un objectif de contrôle interne à satisfaire.

Les risques sont donnés par l'audit mais restent à être validés, voire complétés par les experts des domaines lors de la phase étude.

Le TaRi se remplit de gauche à droite. Ce remplissage est le support d'un raisonnement où chaque colonne est affinée par la colonne suivante, et inversement chaque colonne se déduit de la colonne précédente. Chaque colonne $n + 1$ découle de la n , la précise, la concrétise. Au fur et à mesure qu'on va vers la droite, on a de plus en plus de lignes.

Tableau 6.1 – « On commence par les finalités/objectifs de contrôle interne (1) puis les scénarios d'empêchement (2)... »



Finalités/ objectifs de CI ... du stade/ opération/ élément	Empêchements Risques que la finalité ne soit atteinte	Points de contrôle Étapes clés du CI obser- vables	Impact/risque si étape clé défaillante/ déficiente	Bonnes pratiques de CI Moyens, ressources...
« Être sûr que telle finalité de l'organi- sation sera atteinte, que tel aspect/étape du processus audité est sous contrôle et maîtrisé »	Scénarios de risques : que peut-il se passer ?	Points de passage obligés, concrets, obser- vables : objets à contrôler		
1	2	3	4	5

Un risque (scénario d'empêchement) = 1 ligne (souvent plusieurs lignes pour un objectif)

Un risque (scénario d'empêchement) = 1 ligne (souvent plusieurs lignes pour un objectif)

Finalités : objectifs de contrôle interne, « être sûr que »

Les investigations de l'audit portent sur un « domaine » – on peut également désigner le domaine par le vocable « processus » – identifié par sa *finalité* (ex. : le domaine des achats-fournisseurs dont la finalité est d'acheter des biens ou des services pour la satisfaction de clients finals, internes ou externes). Pour satisfaire à une finalité, des activités sont déroulées dans un ordre chronologique ; on peut parler de sous-processus ou de stades chronologiques. Ces activités sont identifiées par des « verbes d'action » (ex. : pour satisfaire à la finalité acheter, il faut exprimer un besoin, valider un besoin conforme aux besoins de l'entreprise, rechercher des fournisseurs, contractualiser avec un

fournisseur – commander –, suivre la commande, réceptionner les matériels ou les prestations commandées...).

Modalités pratiques : pour une étape, un domaine ou une opération, on aura une ou deux finalités, exceptionnellement trois. Si l'on en a davantage, c'est qu'on a regroupé divers étapes, domaines ou opérations ou fait un découpage trop grossier.

Quand on a plusieurs finalités, il faut les traiter séparément.

Enfin et surtout, *les finalités doivent être des objectifs de contrôle interne* : « être sûr que », et non des actions de contrôle (s'assurer) ni le but opérationnel de l'étape, de l'opération, du sous-processus ou du domaine.

Scénarios d'empêchement : risque que la finalité ne soit pas atteinte

Pour chaque finalité, il faut imaginer ce qui peut se passer et décrire les empêchements possibles *via* des scénarios. Il y a presque toujours plusieurs empêchements pour une même finalité.

Modalités pratiques : les empêchements sont des causes potentielles de non-atteinte de la finalité, des « risques que » la finalité ne soit pas atteinte, et non des conséquences ou impacts, des « risques si » elle n'est pas atteinte.


Quand on a plusieurs empêchements, il faut les traiter séparément sur le même tableau.

On pourra s'appuyer sur des ouvrages spécialisés traitant de scénarios de risques (empêchements). Ci-après un exemple de typologie identifié dans un des cahiers de la recherche de l'IFACI :

- empêchement *social* (grève, revendications, accidents du travail, instabilité de l'emploi, *turnover*, politique de rémunération) ;
- empêchement *financier* (détournement de fonds, gestion des fonds inefficace, mauvaise évaluation des provisions, signature non autorisée, cours boursier surcoté) ;
- empêchement *informatique* (sinistre informatique, absence de documentation des programmes, obsolescence du matériel, manque de formation des utilisateurs, fraude sur fichier) ;

- empêchement *technologique* (non-protection du savoir-faire, contrefaçon, formation inadaptée du personnel, non-optimisation du processus de production) ;
- empêchement *matériel* (incendie, inondation, attentat, vol, dégradation de l'outil de travail) ;
- empêchement *transport* (des biens, des fonds, des informations, des personnes) ;
- empêchement *commercial* (mauvaise anticipation de la concurrence, conditions de vente non respectées, absence de prévisions, publicité inadaptée) ;
- empêchement *politique* (embargo sur les produits, guerre, réglementation protectionniste, confiscation de personnes) ;
- empêchement *écologique* (pollution, destruction) ;
- empêchement *juridique* (non-respect des obligations légales, non-respect d'engagement pris, contrat mal négocié) ;
- empêchement *responsabilité civile* (mauvaise qualité du produit, mauvais état des bâtiments, absence d'assurance).

Tableau 6.2 – « ... on continue par les points de contrôle (3) »



Finalités/ objectifs de CI ... du stade/ opération/ élément	Empêchements Risques que la finalité ne soit atteinte	Points de contrôle Étapes clés du CI obser- vables	Impact/risque si étape clé défaillante/ déficiente	Bonnes pratiques de CI Moyens, ressources...
« Être sûr que telle finalité de l'organisation sera atteinte, que tel aspect/ étape du processus audité est sous contrôle et maîtrisé »	Scénarios de risques : que peut-il se passer ?	Exemples de critères de contrôle : Exactitude Exhaustivité Autorisation Délai Suivi		
1	2	3	4	5

Points de contrôle : étapes clés du contrôle interne, observables

Pour chaque empêchement, les points de contrôle décrivent ce que l'auditeur va contrôler (ce sera repris dans le programme de vérifications, puis dans les constats), donc la réalité (ou la vraisemblance) de l'empêchement, d'une manière indiscutable et selon des critères de résultats objectifs et mesurables : exactitude, exhaustivité, autorisation, délai, suivi.

EXEMPLE DE DÉFINITION DES POINTS DE CONTRÔLE OBSERVABLES

Stade « Réception des achats »

Cinq critères de contrôle (métrique binaire) :

exactitude : réceptionner la prestation ou la marchandise conformément aux termes de la commande et de la réalité ;

exhaustivité : réceptionner toutes les livraisons ou prestations commandées (toutes et sans doublon) ;

autorisation : valider la réception par une personne habilitée (habilitations, preuves, obligations légales) ;

délais : réceptionner dès la mise à disposition de la marchandise ou de la réalisation de la prestation ;

suivi : cela produit l'effet attendu.

S'assurer que – ou être sûr que – tous les besoins exprimés (exhaustivité) font l'objet d'une validation par des personnes habilitées (autorisation) dans des délais permettant de satisfaire la date de livraison (ou de réalisation de la prestation).

Tableau 6.3 – « ... on précise les impacts ou conséquences possibles (4) »



Finalités/ objectifs de CI ... du stade/ opération/ élément	Empêchements Risques que la finalité ne soit atteinte	Points de contrôle Étapes clés du CI observables	Impact/risque si étape clé défaillante/ déficiente	Bonnes pratiques de CI Moyens, ressources...
« Être sûr que telle finalité de l'organisation sera atteinte, que tel aspect/étape du processus audité est sous contrôle et maîtrisé »	Scénarios de risques : que peut-il se passer ?	Exemples de critères de contrôle : Exactitude Exhaustivité Autorisation Délai Suivi	Image Éthique Financier ...	
1	2	3	4	5

Impacts : risques si une étape clé du contrôle interne est défaillante ou déficiente

Il s'agit bien de la conséquence de la défaillance/déficiência d'une étape clé du contrôle interne, telle qu'indiquée dans la colonne précédente et qui sera révélée par les travaux de contrôle.

L'impact s'apparente à des conséquences induites si un objectif de contrôle n'est pas satisfait (ex. : risque financier, risque responsabilité civile).

EXEMPLE D'IDENTIFICATION DES IMPACTS CORRESPONDANTS

Stade « Réception des achats »

Rechercher les conséquences induites par un critère de contrôle non satisfait : métrique quantitative.

Exemple :

réceptionner une marchandise non réelle ou non conforme aux termes de la commande peut induire une fraude ou l'insatisfaction du client final ainsi qu'un surcoût supporté par l'organisation ;


ne pas réceptionner toutes les livraisons/prestations commandées peut induire des litiges avec les fournisseurs et une mauvaise évolution des stocks ;

laisser valider la réception par une personne non habilitée favorise la collusion et la fraude ;

réceptionner tardivement peut générer des litiges avec les fournisseurs et une comptabilité fausse (sous-estimation des charges à payer).

Quels problèmes risque-t-on de rencontrer et qu'entraîneraient-ils ?

Tableau 6.4 – « ... et on termine par les bonnes pratiques de contrôle interne souhaitables (5) »



Finalités/ objectifs de CI ... du stade/ opération/ élément	Empêchements Risques que la finalité ne soit atteinte	Points de contrôle Étapes clés du CI observables	Impact/ risque si étape clé défaillante/ déficiente	Bonnes pratiques de CI Moyens, ressources...
« Être sûr que telle finalité de l'organisation sera atteinte, que tel aspect/ étape du processus audité est sous contrôle et maîtrisé »	Scénarios de risques : que peut-il se passer ?	Exemples de critères de contrôle : Exactitude Exhaustivité Autorisation Délai Suivi	Image Éthique Financier ...	Adoptées Adaptées Disponibles Performantes
1	2	3	4	5

Bonnes pratiques : moyens du contrôle interne, ressources

Les bonnes pratiques décrivent ce qu'en général les audités doivent faire, les moyens et méthodes pour éviter un empêchement (colonne 2).

Ces ressources sont regroupées classiquement en trois grandes familles :

- les **ressources humaines** (l'agent qui exprime un besoin, le responsable qui valide le besoin) ;
- les **ressources matérielles** (sur quel support est saisi et validé le besoin) ;
- les **ressources immatérielles** (notes d'organisation, guide des procédures, informations indispensables : quantité, prix unitaire, budget).

L'ensemble de ressources souhaitées donne l'assurance que l'activité est maîtrisée (réalisation du verbe d'action et respect des critères de contrôle) et que les risques sont sous contrôle. Une ressource mal adaptée devient la cause de la non-réalisation d'un verbe d'action, la non-réalisation d'un verbe d'action constitue un fait/constat et génère des conséquences. Exemple : une personne non habilitée (cause) valide un besoin non conforme aux besoins de l'entreprise (fait) induisant un surcoût financier (conséquence).

Le renseignement de cette colonne se fait par la prise de connaissance de référentiel existant sur un domaine (note de politique interne ou ouvrage externe traitant du domaine) et en répondant à trois questions génériques : que peut-on faire ? Comment fait-on ? Est-ce bien fait ?

Ce sont de bons conseils mais ils ne sont pas obligatoires, contrairement aux critères des points de contrôle. Leur(s) déficience(s) (non adoptées, non adaptées, non disponibles, non performantes) explique(nt) les défaillances des points de contrôle. Elles seront souvent la source des recommandations.

On a maintenant terminé la partie difficile d'une mission d'audit interne : on a déterminé les « objets auditables » et constitué le référentiel d'audit.

Ceci permettra à l'auditeur d'observer, de constater les pratiques ou caractéristiques réelles et de les comparer au référentiel (caractéristiques souhaitées).

EXEMPLE DE LISTAGE DES MODALITÉS DE FONCTIONNEMENT

Rechercher les bonnes pratiques (éléments constitutifs du contrôle interne) qui assurent, *a priori*, que les risques sont couverts :

- les meilleures ressources (humaines, matérielles, immatérielles) organisées au mieux ;
- les bonnes pratiques dictées par les sachants (experts) ;
- les bonnes pratiques observées par le *benchmark* ;
- les bonnes pratiques relevant des règles de « bon sens ».

Ces bonnes pratiques (ressources) doivent être : adoptées (existantes) – adaptées – disponibles – performantes (métrique qualitative).

Stade « Réception des achats »

Les risques de collusion ou de fraude sont couverts si :

- délégation de pouvoirs (bonne pratique adoptée, ressource existante) ;
- délégation respectant le principe de séparation des fonctions (adaptée) ;
- procédure de subdélégation en cas d'absence du délégué (disponible) ;
- la subdélégation n'est pas « le chef en cas d'absence » (performante).

Quand on effectuera une autre mission similaire, on complétera ce référentiel par l'expérience acquise au cours de la première mission (on a pu oublier des points). L'expérience montre qu'on améliore encore significativement à la troisième, mais marginalement au-delà. Cela devient de plus en plus aisé et rapide !

Pour aujourd'hui, on sait qui on va aller voir sur le terrain et ce qu'on va vouloir regarder.

Les auditeurs ont ainsi terminé leur analyse des **risques « génériques »** au bureau. Ils vont maintenant aller sur le terrain discerner les **risques « spécifiques »** à l'entité auditée.

Focus

Le tableau des risques (TaRi)

Le TaRi est un tableau générique à cinq colonnes qui sert de référentiel convenu entre le demandeur, les audités et les auditeurs pour évaluer la maîtrise des risques.

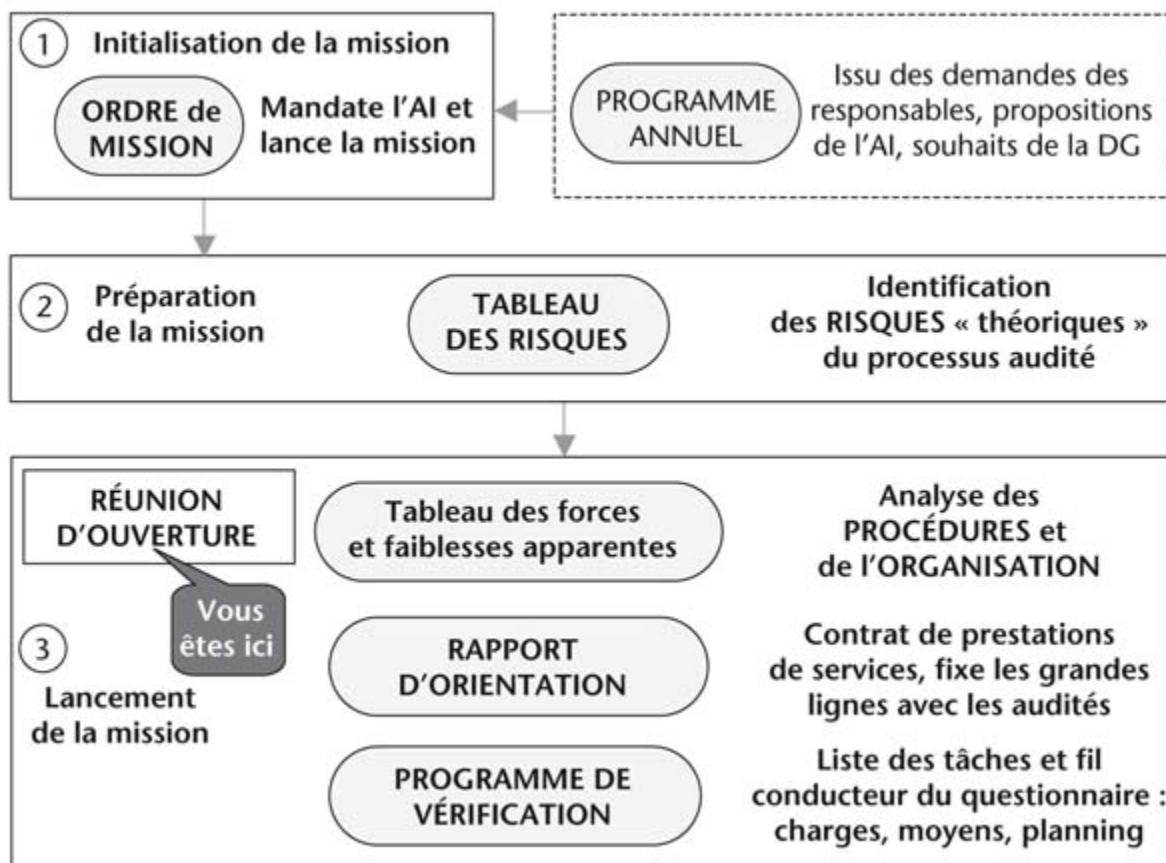
Retour d'expérience

Au-delà des référentiels d'audit types existants pour des missions récurrentes, nombreux sont dorénavant les services d'audit à investir sur l'élaboration de référentiels de risques d'activités ou de processus clés pouvant être audités. À cet égard, le renforcement des entités en charge de prévenir les risques, d'établir des cartographies a été un accélérateur pour pousser les services d'audit à « réfléchir avant d'agir » lors de la mise en oeuvre de la phase d'étude. Les tableaux des risques existants diffèrent le plus souvent sur le nombre de colonnes et en particulier sur la formalisation de la description des risques (souvent une seule colonne centrée sur les impacts, ou sur une approche probabilité/gravité).

L'évolution méthodologique visant à décrire le risque en trois dimensions (empêchements, points de contrôle et impacts) est une aide significative pour l'auditeur afin de l'aider à cerner les points forts et les faiblesses apparentes de l'organisation auditée.

LA RÉUNION D'OUVERTURE OU D'INSTALLATION DE L'ÉQUIPE

La phase d'analyse des risques spécifiques à l'entité auditée s'effectue sur le terrain. Il est souhaitable qu'elle commence par une réunion de présentation auditeurs/audités (encadrement) : la réunion d'ouverture ou d'installation de l'équipe.



Son contenu :

- présenter les auditeurs, se faire présenter les responsables audités et l'activité ;
- clarifier le rôle de la fonction audit interne et son objectif, et décrire la place du service dans l'entreprise (à moins que cela soit

déjà bien connu des interlocuteurs pour avoir été fait récemment) ;

- expliquer les circonstances de la mission, pourquoi ici et maintenant ; c'est un point psychologiquement très important. Il s'agit de dissiper les fantasmes de culpabilité qu'entraîne la venue de l'audit ;
- annoncer le déroulement prévisionnel de la mission ; c'est l'autre point psychologiquement très important, il s'agit d'habituer les audités à l'idée qu'ils sont des acteurs et non des victimes ;
- affiner la logistique et programmer les premiers entretiens.

On peut utilement s'appuyer sur un schéma récapitulatif et quelques *slides* pour rendre la réunion plus attractive et engageante pour les parties prenantes.

FICHE PRATIQUE

La réunion d'ouverture/installation de l'équipe

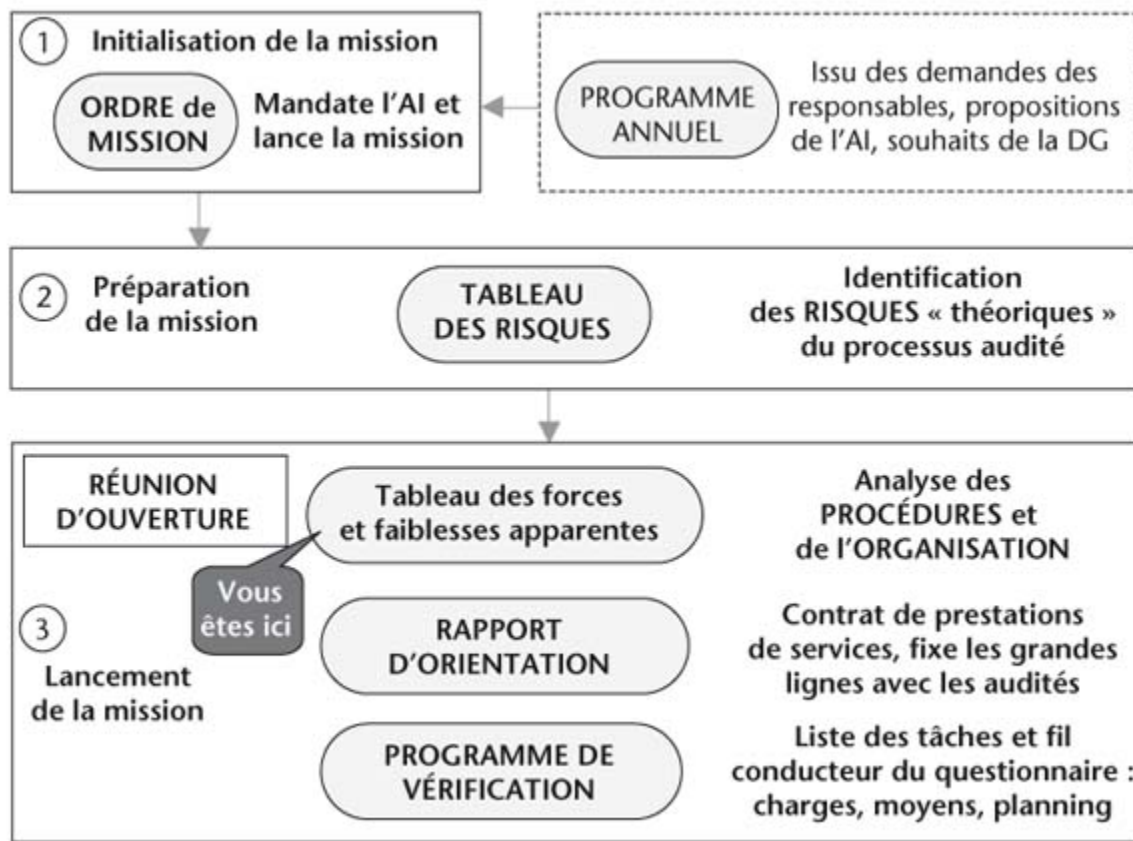
Participants

- Le chef de mission + éventuellement le responsable de l'audit interne
- Les auditeurs
- Le « directeur des audités »
- Les chefs des services audités

Cinq points à aborder

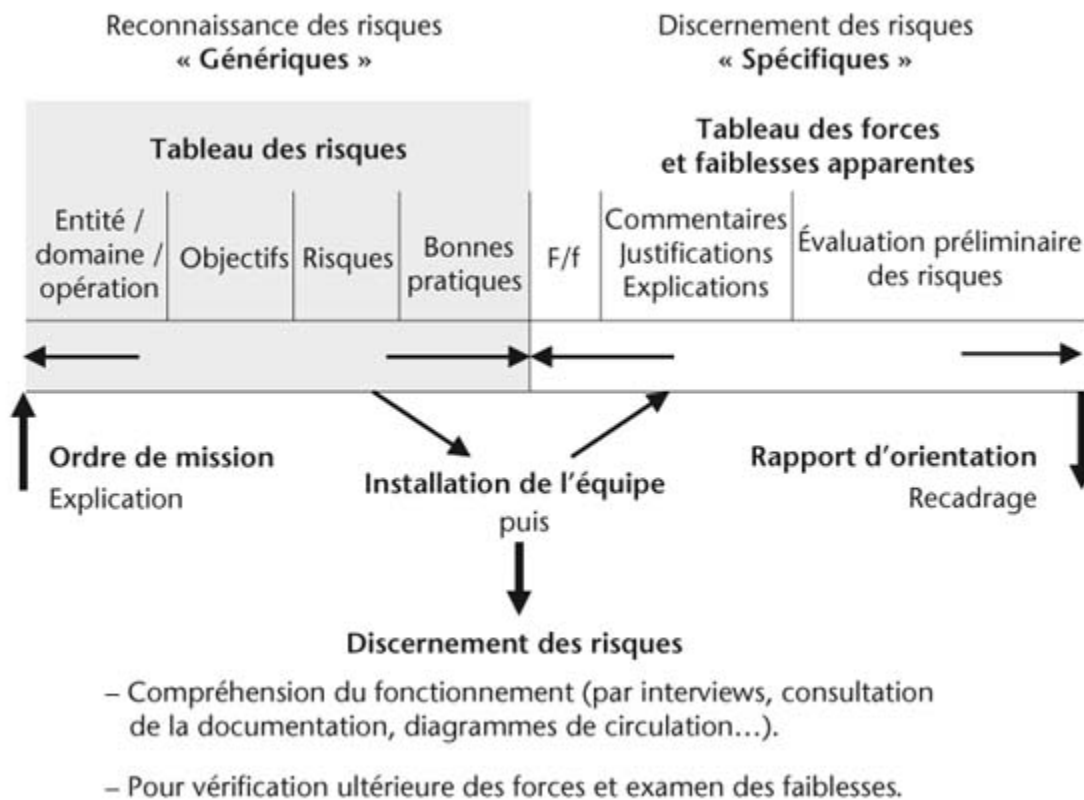
1. Présenter les auditeurs (notamment l'expérience), se faire présenter les audités.
 2. Exposer/rappeler l'audit interne et sa place dans l'organisation.
 3. Expliquer les circonstances de la mission : pourquoi ici et maintenant.
 4. Annoncer le déroulement prévisionnel de la mission, insister sur les échanges avec les audités.
 5. Affiner la logistique (téléphone, mail, bureau...) et prendre les premiers rendez-vous.
- Habituer les audités à l'idée qu'ils sont des acteurs et non des « victimes » de la mission.

L'ANALYSE DES FORCES ET FAIBLESSES



Conditionnant le reste de l'intervention, cette phase d'analyse des risques, dont dépendront la nature et le dosage des contrôles effectués ultérieurement, fait l'objet d'une réflexion approfondie par tous les membres de l'équipe et les risques sont matérialisés en s'appuyant sur le tableau de risques élaboré précédemment. **Elle a pour objectif de faire un état des lieux des forces et faiblesses réelles ou potentielles de l'entité ou du domaine audité afin d'orienter les travaux détaillés.** L'auditeur veillera aux éléments d'appréciation des enjeux et de la maîtrise de l'activité qui sont déterminants pour la suite de la mission ; notamment les données quantitatives permettant d'estimer l'importance des enjeux (ex. : montant des dépenses de prestations fournit par la comptabilité ou par les principaux indicateurs de gestion inhérents à l'activité – dépenses de prestations intellectuelles – et indicateurs de contrôle interne).

Figure 6.2 – Le tableau des risques (TaRi) se prolonge par le tableau des forces et faiblesses apparentes (TFfA)



La phase d'analyse des risques se mène essentiellement par des entretiens, sans tests autres que de bonne compréhension. Il s'agit de comprendre l'organisation et le fonctionnement de l'entité ou des entités auditée(s) – les « diagrammes de circulation » (*flow charts*) sont souvent une bonne technique – pour identifier les forces et faiblesses apparentes et orienter les travaux de vérification ultérieurs.

Certains services d'audit disposent des moyens suffisants pour vérifier tous les risques identifiés dans l'étude préliminaire. Cependant, dans le cas plus habituel d'une recherche d'efficacité, l'apparence d'une force ou d'une faiblesse, et le degré de confiance qu'a l'auditeur quant à la réalité de cette force ou faiblesse, vont guider ses travaux ultérieurs :

- confirmer les forces critiques non certaines ;
- ne pas perdre de temps sur les autres forces (forces certaines et forces probables mais non critiques) ;

- étudier et résoudre les faiblesses graves ;
- ne pas perdre de temps sur les autres faiblesses.

Focus

Le tableau des forces et faiblesses apparentes (TFfA)

Le TFfA conclut l'étape de discernement des risques préparée par le référentiel de risques (TaRi). Il a pour objectif de faire un état des lieux des forces et faiblesses réelles ou potentielles de l'entité ou du domaine audités afin d'orienter les travaux détaillés.

Retour d'expérience

Nous avons noté que des services d'audit justifient la non-réalisation de ce produit méthodologique par souci de gagner du temps à la phase d'étude et de privilégier les vérifications et tests de terrain.

Il y a lieu de bien considérer que le TaRi et le TFfa ne font qu'un dès lors que le premier pose les risques théoriques/génériques de l'activité et le deuxième exprime l'opinion de l'auditeur après analyse rapide des risques potentiels sur le terrain.

Le but du TFfa est de limiter les travaux sur chaque mission pour faire davantage de missions et mieux couvrir l'entreprise.

LE RAPPORT D'ORIENTATION OU LA NOTE DE CADRAGE

À la fin de la phase d'étude de la mission et juste avant que ne démarre la phase de vérification de l'audit, un document synthétique présente dans un rapport d'orientation (RdO) les objectifs poursuivis et zones de risques que les auditeurs vont examiner. Il délimite ainsi précisément le champ de l'intervention. Il est à noter que la direction de l'audit pourra à ce stade proposer de ne pas continuer la mission si en fin d'étude préliminaire l'enjeu ne s'avérerait pas réel ou pertinent.

Nous recommandons de l'envoyer au demandeur de la mission pour avis, puis de le présenter aux audités pour information. Il est donc formulé dans leur langage.

C'est une formulation et une précision de l'ordre de mission (on passe d'ailleurs d'une demi-page à deux pages), et certains l'appellent « recadrage ».

FICHE PRATIQUE

Élaboration du rapport d'orientation (RdO)

- **Pour être pertinent** : le RdO reprend les conclusions retenues du tableau des risques : forces/faiblesses apparentes + préoccupations du management. Il est discuté avec les principaux responsables audités et le demandeur.
- **Pour être percutant** : le RdO est formulé en objectifs à atteindre pour le client et rédigé en faisant abstraction des travaux d'audit qu'il implique. Il est bref : de 1 à 3 pages.
- **Pour être un « contrat »** auditeur/audités (et demandeur) : utiliser des mots-clés.

Le rapport d'orientation assure donc la pertinence des travaux :

- par la concertation avec les principaux responsables audités et le demandeur : c'est le contrat que l'audit interne passe avec eux ;
- par l'objectivité de la démarche : découpage, objectifs, risques, bonnes pratiques, analyse des risques (survol), ciblage/choix..

FICHE PRATIQUE

Les mots-clés du rapport d'orientation

On commencera chaque phrase du rapport d'orientation par :

- « **S'ASSURER DE** » ou « **VÉRIFIER QUE** » quand on s'engage à donner une assurance qu'un point est sous contrôle : à fournir une opinion binaire (oui/non, ça marche ou ça ne marche pas) ;
- « **APPRÉCIER** » quand on s'engage à émettre une opinion qualitative après étude, ou « **REVOIR** » quand on s'engage à faire l'étude mais n'émettre d'opinion que s'il y a lieu ;
- « **ÉVALUER** » quand on s'engage à fournir une information quantitative mais *a priori* sans émettre d'opinion, ou « **ANALYSER** » quand on s'engage à faire l'étude mais pas à obtenir des résultats ;
- « **VOIR S'IL Y A LIEU D'APPROFONDIR** » quand on hésite et qu'on ne s'engage à rien !

Focus

Le rapport d'orientation (RdO) ou la note de cadrage

Le RdO ou la note de cadrage définit et formalise les axes d'investigation de la mission et ses limites. Il les exprime en objectifs à atteindre par l'audit pour le demandeur et les audités, dans leur langage.

Retour d'expérience

Dans le cadre d'audits récurrents, les services d'audit disposent d'un rapport ou d'une note d'orientation standard. Pour les nouveaux thèmes d'audits, le principe méthodologique est appliqué mais la différenciation par des verbes d'action est rare, sans doute en lien avec la difficulté de s'engager sur les forces et faiblesses apparentes dès la phase d'étude (*cf. supra*).

Tableau 6.5 – La phase d'étude aboutit aux étapes suivantes

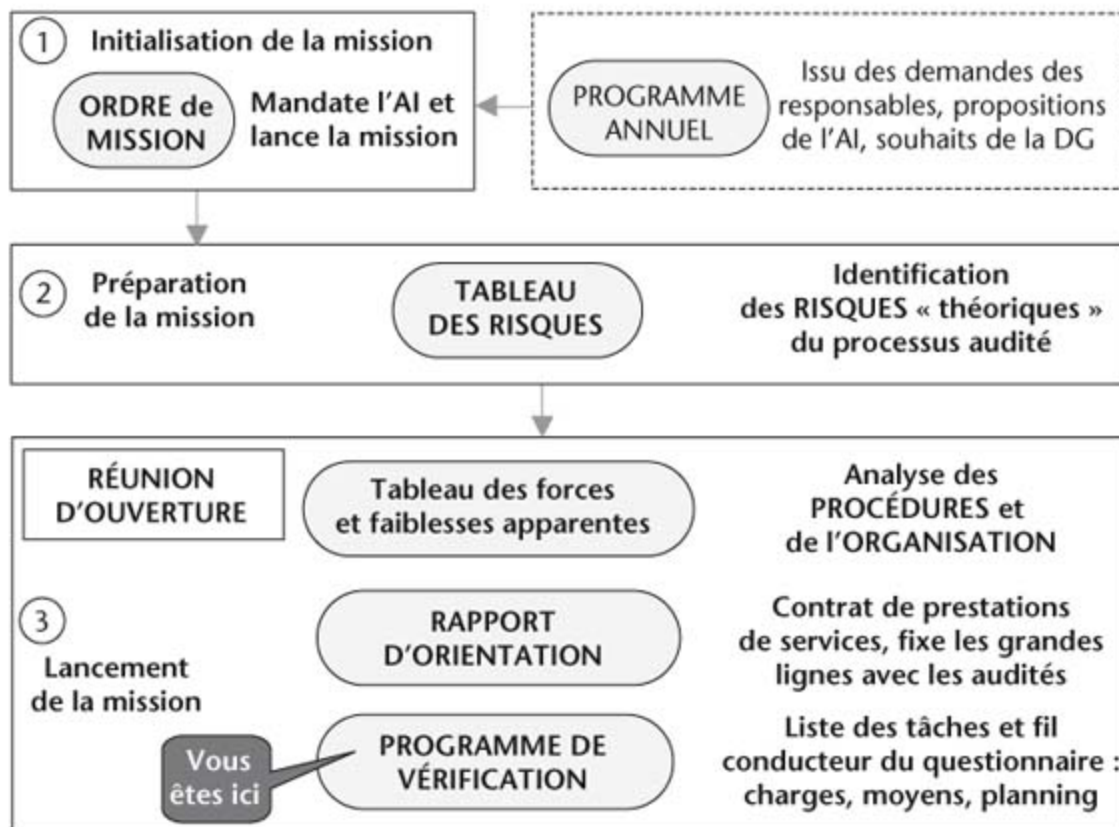


LE PROGRAMME DE VÉRIFICATION

C'est sur la base du rapport d'orientation que s'établit le programme de vérification de l'équipe d'audit, le budget et le planning d'affectation des tâches, puis des feuilles de couverture.

Le programme de vérification, souvent appelé programme de travail, est la gamme de fabrication à mettre en œuvre pour atteindre

les objectifs du rapport d'orientation. C'est un document interne au service d'audit interne, destiné à définir, répartir, planifier et suivre les travaux des auditeurs. La matérialisation de la répartition s'effectue par un tableau des tâches et un état dit « BP » (*budget planning*). Il indique la liste des tâches à effectuer, des investigations à mener, des questions à poser, des points à voir, des procédures à rechercher.



Les travaux sont décomposés en tâches distinctes pour pouvoir être attribués aux auditeurs. Cependant, le programme de vérification n'est ni une obligation, ni une excuse : l'auditeur garde une « marge de manœuvre » et devra faire preuve d'initiative et de jugement.

Le programme de vérification est un document majeur qui procure cinq bénéfices :

1. il assure le responsable de l'audit interne que toutes ses préoccupations sur le sujet ont été prises en compte et qu'il y sera répondu : c'est le contrat entre lui et l'équipe chargée de la mission ;

2. il permet au chef de mission d'évaluer les tâches que cela implique, de les répartir entre auditeurs et d'établir le planning de la mission (puis de le suivre) jusqu'au rapport ;
3. il guide les auditeurs et leur évite de déborder et de « peaufiner » ;
4. il documente le déroulement de la mission et sert de tableau synoptique : qui a effectué le travail ? Quand a-t-il été terminé ? Comment s'y est-on pris et qu'a-t-on trouvé (feuilles de couverture) ? Quels problèmes ont été identifiés (FAR) ? ;
5. il capitalise le savoir-faire du service en servant d'exemple et d'inspiration pour d'autres missions : pour les missions récurrentes, il suffit d'adapter le standard à la nouvelle unité.

Focus

Le programme de travail ou de vérification (PdV)

Le PdV est la gamme de fabrication à mettre en oeuvre pour atteindre les objectifs du rapport d'orientation : liste des tâches à effectuer, des investigations à mener, des questions à poser, des points à voir, des procédures à rechercher.

Retour d'expérience

On retrouve fréquemment ce document interne au service d'audit, destiné à définir, répartir, planifier et suivre les travaux des auditeurs. Il permet au chef de mission d'évaluer et de répartir les tâches et d'établir le planning jusqu'au rapport. Il documente le déroulement, sert de table d'orientation et capitalise l'expérience.

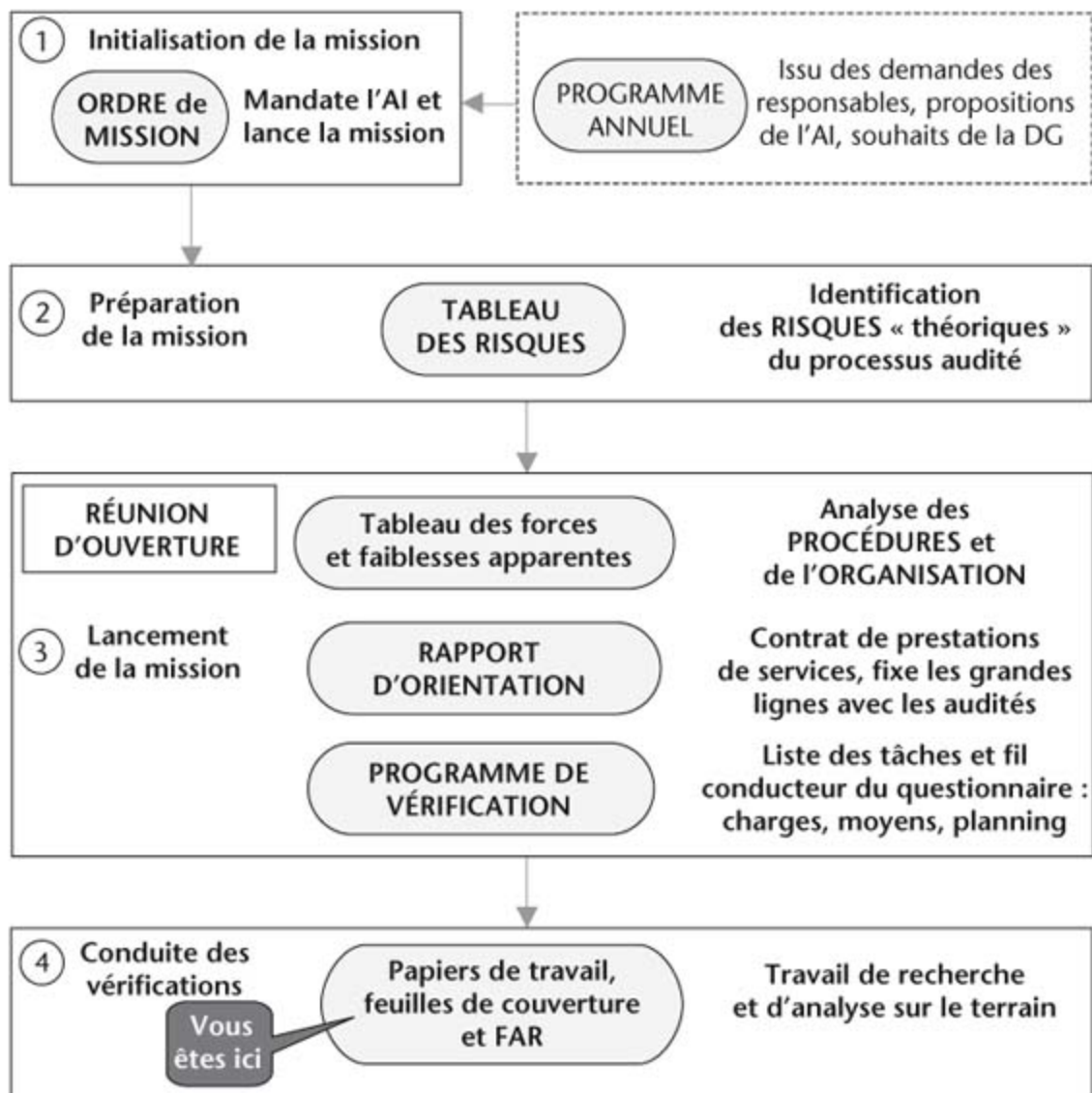
LA CONDUITE DES VÉRIFICATIONS ET LA FORMALISATION DES TRAVAUX DE CONTRÔLE

Les papiers de travail

Les travaux de vérification sont effectués et les informations recueillies sur l'ensemble des points concernés par les objectifs de la mission. Ces informations doivent être suffisantes, fiables, pertinentes et utiles pour fournir une base saine et sûre aux constatations et recommandations.

Le travail sur le terrain consiste à conduire les contrôles prévus au plan de travail :

- mener des enquêtes, tracer des diagrammes, réaliser des observations physiques, effectuer des rapprochements et reconstitutions, interroger des fichiers informatiques et établir les papiers de travail, tout ceci :
 - en restant à l'écoute des élargissements, approfondissements qui peuvent apparaître intéressants ;
 - et en se posant en permanence la question de savoir s'il ne serait pas plus rentable de réorienter le travail (le résultat recherché apparaît impossible à obtenir ; il est déjà suffisamment atteint sans avoir effectué tous les travaux prévus) ;
- périodiquement et au moins à la fin de chaque section, présenter ses papiers de travail avec suggestions de recommandations au chef de mission et au superviseur. Puis les discuter avec les audités concernés ;
- à la fin de chaque section, référencer les papiers de travail pour archivage ultérieur.



FICHE PRATIQUE

Les papiers de travail (PdT)

Objectifs

- Matérialiser la production et la progression de la mission
- Recueillir les informations obtenues
- Identifier et documenter les faiblesses relevées
- Alimenter les discussions avec les audités
- Étayer le rapport
- Valider les conclusions et les recommandations

- Faire superviser l’avancement et les résultats de la mission
- Fournir des références aux missions futures

Conseils pratiques

- Style dépouillé, voire télégraphique
- Au « crayon » ou sous un logiciel de traitement de texte
- Aéré pour compléments
- Pré-imprimé, coloré
- Légende des « tick marks »
- Différencier les faits des commentaires et opinions
- Reprise des PdT antérieurs

La feuille de couverture

Ce document, établi en deux temps, décrit les modalités de mise en œuvre d’une tâche définie dans le programme de vérification, puis met en évidence les conclusions qui en ont été tirées. Avant d’effectuer une tâche, par exemple un test ou une interview, l’auditeur en spécifie les modalités sur sa feuille de couverture et en convient avec le chef de mission :

- pour le test : sources, périodes à prendre en compte, format des documents et/ou tableaux d’exploitation..., format du document et/ou tableau de résultats ;
- pour l’interview : personnes à interviewer, lieux, dates, durées, guide d’interview (les questions).

Le chef de mission, *a priori* plus expérimenté, pourra souvent conseiller l’auditeur et rendre la tâche plus aisée et plus rapide (notamment choix des documents sources) ou le format des conclusions plus directement utilisable.

Après les travaux détaillés, tests et interviews dans notre exemple, l’auditeur rédige ses conclusions sur la feuille de couverture.

Elle est ainsi un document particulièrement synthétique qui facilite la constitution du dossier et la supervision :

- la supervision « quotidienne » qui s’assure que les conclusions sont étayées (approbation de la méthode utilisée, allers-retours entre la feuille de couverture et ses papiers de travail détaillés) ;
- la supervision « globale » qui vise à dégager les conclusions de la mission au fur et à mesure de l’avancement des travaux (ceci peut

aussi être fait avec les FAR : voir paragraphe suivant), sans aller plus en détail que les feuilles de couverture.

La feuille de couverture apporte des gains de temps et de productivité. Elle réduit l'étendue du travail nécessitant concertation entre les auditeurs : jusqu'au programme de vérification ils travaillent ensemble. À partir de la feuille de couverture, ils travaillent en parallèle.

Les feuilles de couverture sont souvent produites en « temps masqué », à un moment où l'auditeur aurait soudainement du temps disponible : une réunion a été annulée, écourtée ou retardée ; il a raté son train et attend le suivant...

Elles sont produites au fur et à mesure des besoins, ce qui évite d'établir les spécifications des actions devenues caduques, soit parce que d'autres actions se sont avérées suffisantes pour conclure, soit parce qu'un point a été abandonné.

Exemple de feuille de couverture de test

Audit du recouvrement de créances de XYZ Test sur les délais de mise à jour du fichier clients	E 500 Établi par JPB le 16/12/aaaa	Réf. PdT	Réf. FAR
BUT Vérifier les délais de mise à jour du fichier clients tenu à V. à partir des règlements arrivant à U. MODALITÉS D'EXÉCUTION <ul style="list-style-type: none"> • Déterminer 3 périodes dans le dernier mois écoulé (début, milieu et fin de mois) correspondant à la colonne 1 sur la feuille de test. • Se référer au bordereau manuel envoyé par U. à V., décomposer les soldes à partir des justificatifs joints au bordereau et déterminer le nombre de règlements globaux (colonne 3). 		B 2.3	
<ul style="list-style-type: none"> • Relever la date sur le listing V. (colonne 2). • Vérifier sur le listing que les montants enregistrés en $n + 1$ correspondent aux nombres de règlements globaux envoyés par U. en n (en fait compter le nombre de code 22 sur le listing) (colonne 4). • Vérifier sur écran que les règlements non repérés sur le listing ont été résolus dans la journée (colonne 5). • Totaliser et déterminer les pourcentages du nombre de montants enregistrés/non enregistrés. Amont			
RÉSULTATS : voir papiers de travail Aval CONCLUSIONS : <ul style="list-style-type: none"> • Test satisfaisant car le nombre de montants enregistrés bordereau/listing est équivalent. • Les règlements non repérés sur le listing sont résolus dans la journée dans 87 % des cas. • Seul un problème de transmission par la Poste existe. 		E501 à E502	Non Non Far 7

FICHE PRATIQUE

La feuille de couverture (FdC)

Établie en deux temps

- Avant : le but de l'action (PdV) et les modalités.
- Après : les résultats et conclusions (+ modifications éventuelles), des réponses précises, concises et contrôlables.

Intérêt : gains de temps

- Permet d'alléger et donc d'accélérer le programme de travail.
- Réduit l'étendue du travail nécessitant concertation.

- Évite d'établir les spécifications des actions retenues devenues caduques.
- Accroît la productivité car établie en « temps masqué ».
- Facilite la constitution du dossier synthétique et la supervision.

Focus

La feuille de couverture (FdC)

La FdC est un document établi en deux temps, avant puis à la fin d'une tâche définie dans le programme de vérification. Elle spécifie les modalités de mise en oeuvre, puis met en évidence les résultats obtenus et les conclusions qui en ont été tirées.

Retour d'expérience

La feuille de couverture comporte donc uniquement la méthode utilisée et les résultats et conclusions, le reste ne figurant que sur les papiers de travail produits au cours de la tâche. Elle est très inspirée des supports utilisés par les cabinets d'audits externes (*finding sheet*) ou de conseil.

En audit interne, on retrouve fréquemment ces informations soit en complément du programme de travail ou directement dans les papiers de travail. Un effort doit être entrepris pour développer la feuille de couverture au sein des services d'audit. En effet, elle apporte des gains de temps et de productivité. Elle réduit l'étendue du travail nécessitant concertation entre les auditeurs : jusqu'au programme de vérifications, ils travaillent ensemble. À partir de la feuille de couverture, ils travaillent en parallèle.

LA FICHE D'AUDIT ET DE RECOMMANDATIONS (FAR)

La FAR, historiquement appelée FRAP (feuille de révélation et d'analyse de problèmes), est le papier de travail synthétique par lequel l'auditeur présente et documente chaque dysfonctionnement. Elle facilite la communication avec l'audité concerné.

Figure 6.3 – Point d’audit

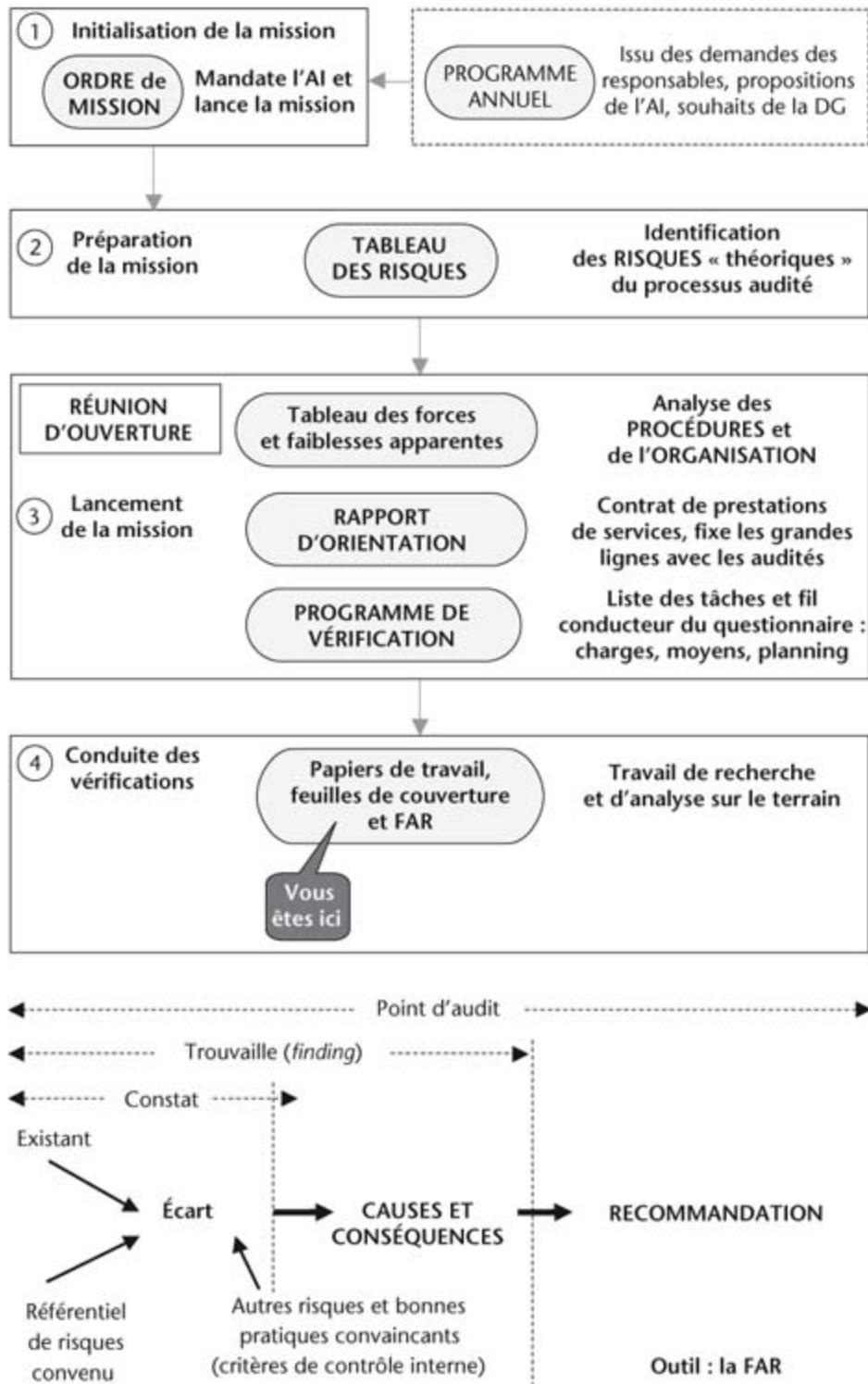



Tableau 6.6 – Le TaRi guide l’élaboration de la FAR



Finalités/ objectifs de CI ... du stade/ opération/ élément	Empêchements Risques que la finalité ne soit atteinte	Points de contrôle Étapes clés du CI observables	Impact/ risque si étape clé défaillante/ déficiante	Bonnes pratiques de CI Moyens, ressources...
« Être sûr que telle finalité de l’organi- sation sera atteinte, que tel aspect/ étape du processus audité est sous contrôle et maîtrisé »	Scénarios de risques : que peut-il se passer ?	Exemples de critères de contrôle : Exactitude Exhaustivité Autorisation Délai Suivi	Image Éthique Financier ...	Adoptées Adaptées Disponibles Perfor- mantes
1	2	3	4	5

**Les rubriques du tableau des risques initial
préfigurent les 5 rubriques de la FAR :**



La méthodologie employée consiste à étudier le fonctionnement réel des opérations : repérer les constats significatifs, déterminer leurs causes, démontrer les conséquences et proposer des moyens d’amélioration.

Après chaque étape de travail, des conclusions partielles sont rédigées par l’auditeur. Ce sont les constats des déficiences identifiées.

L’ensemble des points fait l’objet d’un regroupement par domaine ou centre d’intérêt et des conclusions sont arrêtées par les auditeurs qui

les restituent sous forme de fiches synthétiques, dénommées « fiches d'audit et de recommandations » (FAR). Ces fiches sont présentées aux principaux responsables concernés afin d'enregistrer leurs réactions et discuter à chaud des principales recommandations que les auditeurs seront amenés à faire dans le rapport d'audit.

Fiche d'audit et de recommandations (FAR)

FAR n°...		
Papier de travail :		
Problème : <i>[Formulation synthétique, autonome, percutante]</i>		
Constats : <i>[Éléments de preuve]</i>		
Causes : <i>[Explications]</i>		
Conséquences : <i>[Impact/gravité]</i>		
Solution proposée : <i>[Actions à mener]</i>		
Établi par :	Approuvé par :	Validé avec :
Le :	Le :	Le :

Tout dysfonctionnement, y compris un risque non ou mal maîtrisé, que les travaux de l'auditeur ont mis à jour, est formulé sous forme de FAR :

- le « problème » qui le résume en une formulation synthétique, autonome et percutante ;
- les « constats » qui le prouvent ;
- les « causes » qui l'expliquent ;
- les « conséquences » qui le pèsent ;
- les « recommandations » qui le résolvent.

FICHE PRATIQUE

Comment élaborer une FAR ?

1. Commencer par le/ les CONSTATS	Fournir les PREUVES	Les faits doivent avoir été observés (pas de jugement sans preuve).
2. Remonter aux CAUSES	Donner des EXPLICATIONS	Les causes peuvent avoir été constatées ou déduites (des explications trop éloignées des faits affaiblissent l'argumentation et font naître le doute).
3. Pour en déduire les CONSÉQUENCES	Faire percevoir la GRAVITÉ	Les conséquences peuvent être quantifiées ou qualifiées (une gravité contestée dilue les conséquences : valider avec le responsable).
4. Résumer l'ensemble en un PROBLÈME	Provoquer une RÉACTION	Le problème doit énoncer l'objectif compromis, le mal à supprimer (une réaction sans compréhension immédiate = un parasite pervers).
5. Proposer une SOLUTION	Obtenir l'ACTION	La recommandation doit relier le mal et l'objectif. Il faut chercher une solution à résultats rapides.

Quand il fabrique une FAR, l'auditeur commence toujours par les constats. Il les a nécessairement relevés, observés. Ce ne peut pas être un jugement (mais cela peut être introduit par un jugement).

Il complète ensuite les causes et les conséquences, l'ensemble constats + causes + conséquences constituant la « trouvaille ». Les causes et conséquences sont le résultat d'une déduction, et sont aussi parfois constatées. Les conséquences non constatées sont des « risques ».

Toute section du travail de terrain se termine par la mention « FAR n° x » ou « pas de FAR » quand il n'y a pas de problème. Tant qu'il n'a pas établi sa trouvaille, l'auditeur n'a pas fini son travail d'investigation et de réflexion, même s'il a effectué toutes les tâches prévues sur cette section ; inversement, dès qu'il a établi sa trouvaille, il a fini et ce n'est pas la peine d'effectuer les autres tâches.

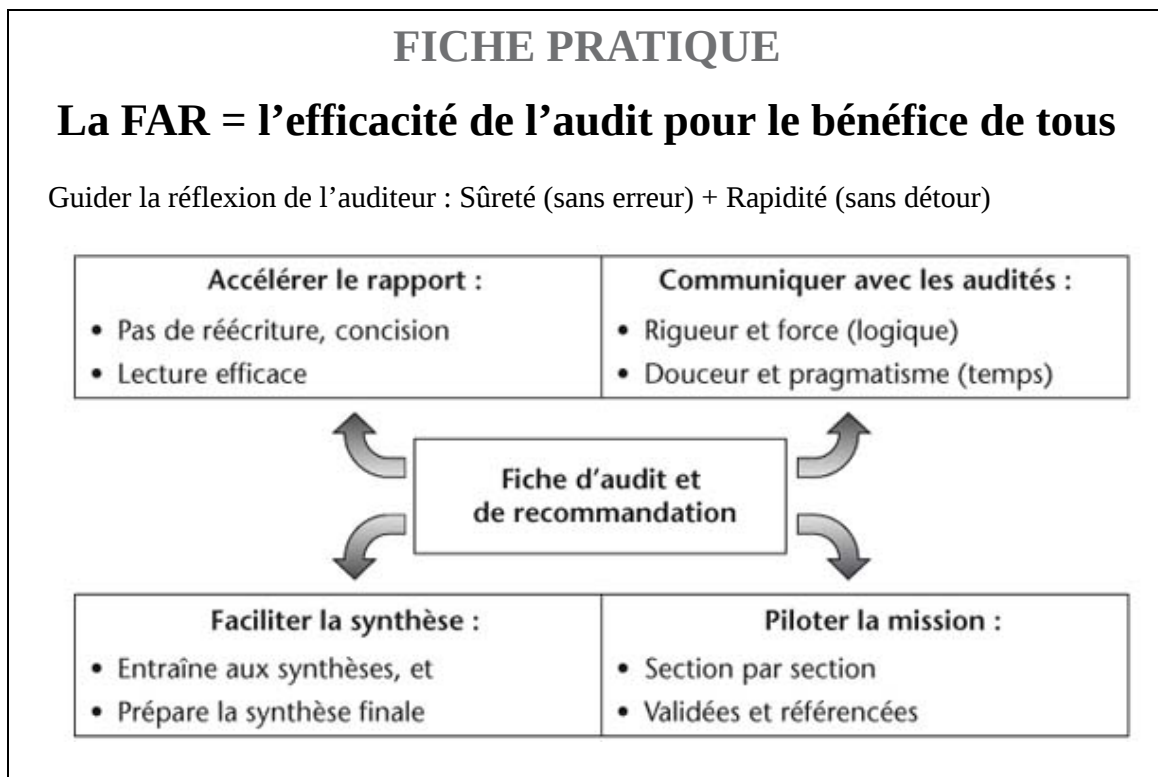
La FAR est ainsi ce qui guide l'auditeur sans erreur ni détour : c'est cela et uniquement cela qu'il a à faire, et il sait comment le faire : 1) faits constatés, 2) causes et conséquences déduites.

La FAR va ensuite servir à communiquer avec l'audité concerné. Pour cela :

- l'auditeur résume la trouvaille et la reformule en un problème synthétique, autonome et percutant, comme une publicité par voie d'affiches ;
- il la fait approuver par son chef de mission, ce qui amène habituellement à une ou des reformulations et à un affinement de la réflexion (l'auditeur seul dans son entreprise tâchera de se trouver un mentor ou laissera quelques jours s'écouler afin « d'oublier » avant de se relire) ;
- il la valide ensuite avec l'audité concerné. Il valide le contenu – constat, déductions, formulation du problème – mais il ne fait pas « avouer et signer » l'audité. Il s'agit d'une discussion de travail reconnaissant l'autorité et la compétence de l'audité, bien avant que tout ceci soit couché dans un rapport qui remontera à la hiérarchie, et cherchant sa coopération pour bâtir une solution.

L'audité, éclairé par l'auditeur quant au problème et à ses constituants, trouve en effet alors plus facilement la solution que l'auditeur. Mais celui-ci ne viendra pas avec une FAR sans solution, uniquement critique : il ébauchera une solution avant d'aller valider sa FAR. Inversement, il ne cherchera pas à élaborer la solution tout seul,

afin de permettre à l'audité de s'approprier le problème et de participer à sa solution.



On procède ainsi, section par section, avec des FAR validées au fur et à mesure avec les audités, et référencées (la mission et le numéro de la FAR, les papiers de travail qui l'étaient, son émetteur, l'approbation par le chef de mission, la personne avec qui on l'a validée). Le pilotage de la mission est grandement facilité.

La synthèse de la mission est grandement facilitée aussi : chaque problème est la synthèse d'une trouvaille, et il suffit de trier les problèmes dans un ordre intéressant pour produire « l'extrait sec » de la mission : l'ossature du rapport (voir le prochain paragraphe).

L'émission du projet de rapport est aussi radicalement accélérée.

Si les FAR sont sur traitement de texte, on constitue, par quelques modifications simples et rapides (24 à 48 heures), l'ossature du rapport et le corps du rapport sans rédaction nouvelle (et ultérieurement les formulaires de recommandation/réponse) : on débarrasse les FAR de leurs mentions administratives, on les trie dans l'ordre de l'ossature, on rajoute les titres des problèmes.

EXEMPLE DE FORMAT D'UNE PAGE DE RAPPORT D'AUDIT

SYSTÈME INFORMATIQUE (réseau micro-ordinateur)

L'absence de procédure ne permet pas de s'assurer de la sauvegarde correcte de l'ensemble des enregistrements comptables.

Constats :

Les copies de sécurité des fichiers de données ainsi que les sauvegardes de travaux mensuels ne sont pas faites systématiquement.

En ce qui concerne les fichiers de données, il y a eu mélange dans les « générations » de copies de sécurité. Il est prévu de sauvegarder périodiquement et alternativement sur les fichiers 1 et 2, mais des inversions ont eu lieu.

Causes :

Il n'existe pas de procédure formalisée décrivant les sauvegardes périodiques et les opérations à effectuer.

Conséquences :

Il n'est pas possible d'éditer le grand-livre avec la totalité des écritures de l'année (perte des écritures de février).

En cas de reprise après incident, la société risque de ne pas avoir la dernière « génération » de données, mais une version plus ancienne, ce qui implique une reprise laborieuse.

Recommandation = le chef comptable devrait :

Formaliser une procédure décrivant les fichiers à sauvegarder, la périodicité des sauvegardes et la technique de sauvegarde.

Si l'on préfère réécrire en « bon français », la tâche est simplifiée. Chaque FAR est « traduite » en : il existe (*tel problème*) qui se manifeste par tels incidents et telles anomalies qui ont été constatées (*les constats*), l'origine en est (*causes*), et cela a comme impact certain ou probable (*conséquences*), cela nécessite (*recommandations*).

Focus

La fiche d'audit et de recommandations (FAR)

La FAR est le papier de travail synthétique par lequel l'auditeur présente et documente chaque risque ou dysfonctionnement à signaler :

- le « problème » qui le résume ; c'est une formulation : elle doit être synthétique, autonome et percutante ;
- les « constats » qui le prouvent ;

- les « causes » qui l’expliquent ;
- les « conséquences » qui le pèsent ;
- les « recommandations » qui le résolvent.

Retour d’expérience

Membres d’un groupe de recherche de l’IFACI dirigé par Olivier Lemant, nous avons adopté ce produit méthodologique dès 1985.

À cette époque, le terme de FRAP avait été retenu pour donner à l’auditeur le moyen de présenter sans détour et avec force le problème et la recommandation et « frapper » les esprits. Cependant, sur le plan de la communication, certains audités recevaient difficilement le terme, y associant un jugement de valeur.

Nous avons retenu pour notre part le terme de FAR, l’associant phonétiquement à un phare qui éclaire sur la voie à suivre et prévient des risques. Ce terme est plus positif et orienté sur des actions de progrès.

De nos jours, les services d’audit ont pour certains adopté des formulations diverses comme « fiche de constat et de recommandation, feuille de synthèse... »

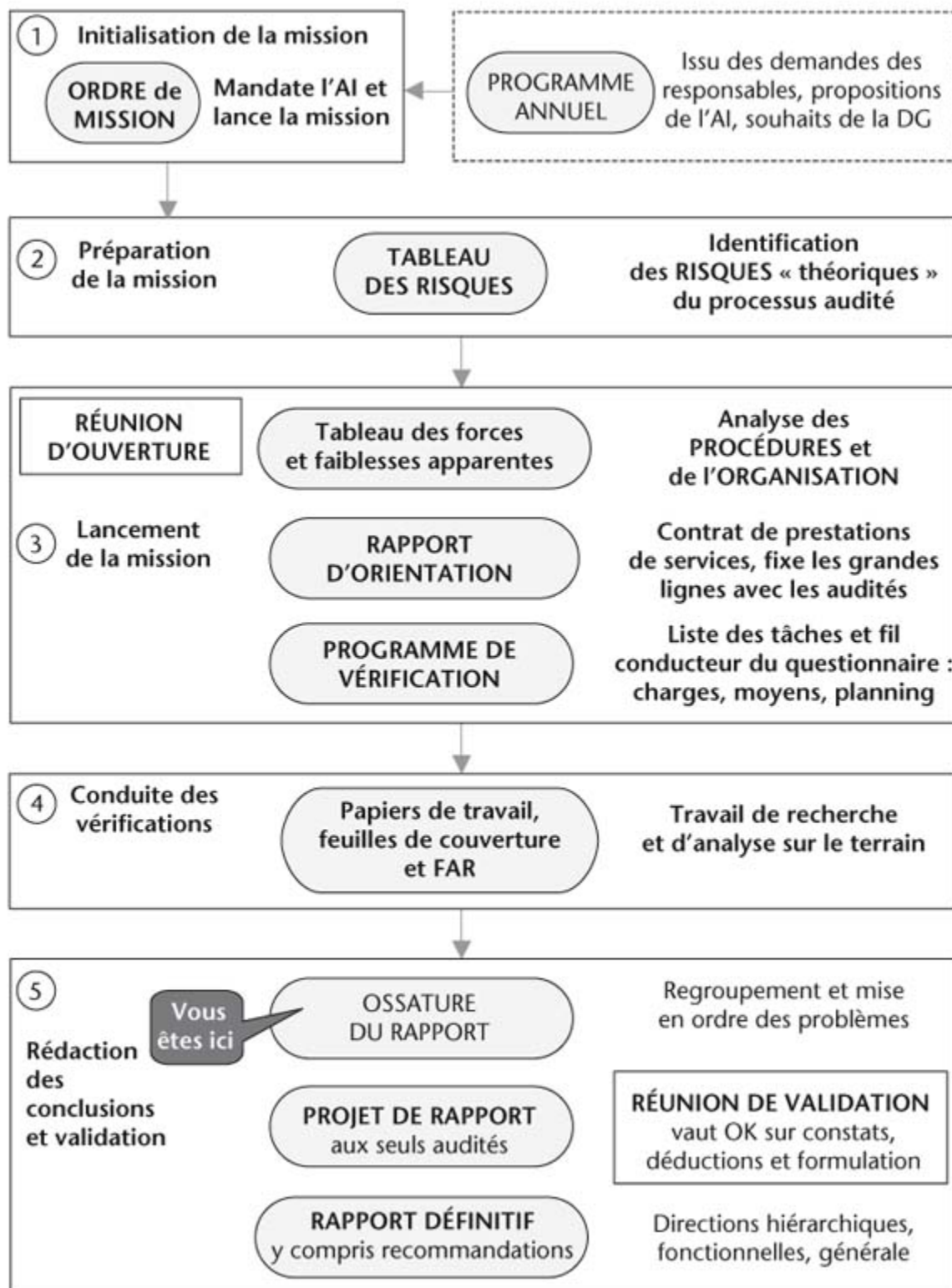
L’esprit des rubriques de la FRAP a été préservé mais on notera que certains services regroupent leurs observations et réflexions dans la seule rubrique des constats, d’autres n’isolent pas systématiquement la ou les causes, ce qui rend délicate la proposition de solutions détaillées et opérationnelles.

Enfin, la pression du temps a conduit les services d’audit à substituer à la puissance analytique de la FAR la volonté de privilégier des présentations synthétiques sous forme de diapositives.

L’OSSATURE DU RAPPORT

L’ossature du rapport (OR) est l’enchaînement des messages que l’audit interne veut délivrer dans le rapport concluant la mission ; elle est élaborée à partir des problèmes figurant sur les FAR (et des conclusions figurant sur les feuilles de couverture).

C’est un petit travail : au cours d’une réunion de synthèse interne à l’équipe des auditeurs, on reprend les énoncés de problèmes figurant en haut de chaque FAR, on les classe dans un ordre qui semble intéressant – par thème, par ordre d’importance – et on rajoute les titres de regroupements sous lesquels ils apparaîtront dans le rapport.



On suivait en effet jusqu'ici une logique de questionnement : celle du rapport d'orientation et du programme de vérification. Certaines questions ont donné des réponses sans grand intérêt, d'autres des réponses très riches. Il faut maintenant pivoter vers une logique de présentation, de points à faire passer (sauf quand on s'impose un plan standard pour effectuer de temps à autre des comparaisons entre unités ou de la même unité dans le temps, sur un thème donné).

Attention : réordonner les points aboutit parfois à fusionner deux FAR pour faire de deux points secondaires un point important (ou à éclater pour clarifier) : c'est une autre raison pour ne pas faire signer les FAR quand on les valide ; il faut pouvoir évoluer.

C'est un travail nécessaire : il faut se forcer à prendre du recul et organiser la réflexion et le discours de l'équipe d'audit avant de rendre compte des travaux et conclusions aux principaux responsables audités, au demandeur et à la direction. Ceci se fait en concertation avec le responsable de l'audit interne et le superviseur.

Attention : le produit de ce petit travail, l'ossature du rapport, est explosif. C'est, et ce n'est qu'une liste de problèmes formulés de manière percutante, qui tient en général sur une page. C'est une page centrée sur les seules faiblesses. Cela ne doit pas sortir du service d'audit interne, sauf sous la forme d'une diapositive que l'on projette (mais dont on ne laisse pas de copies) et autour duquel on parle, en nuancant les critiques, en les replaçant dans leur contexte, et en citant les points positifs.

L'ossature du rapport peut donc ainsi servir de support de présentation, mais pas de table des matières du rapport : elle risquerait d'être copiée et de circuler. Elle sert de guide de montage du corps du rapport, et de guide de rédaction de son résumé.

FICHE PRATIQUE

Pivoter du rapport d'orientation au plan du rapport lors d'une réunion de synthèse interne à l'équipe d'audit

L'ossature du rapport (OR) est l'enchaînement des messages que l'audit interne veut délivrer dans le rapport concluant la mission. Son but est d'organiser la réflexion et le discours de l'équipe d'audit avant de rendre compte de ses conclusions aux principaux responsables audités, au demandeur et à la direction. Elle permet de :

- reprendre tous les problèmes (de manière synthétique, autonome, percutante) ;
- décider ce qu'on veut écrire dans le rapport et ordonner ses idées ;
- établir la liste ordonnée des problèmes avec intertitres.

OR = énoncé des problèmes, classés dans l'ordre désiré pour le rapport, avec titres de regroupements

Pivoter	Ne pas pivoter
D'une logique de questionnement (intellectuelle) à une logique de présentation : - points à faire passer ; - faiblesses relevées par thèmes ; - provisions à passer par montants.	Structure constante, par exemple : - un thème tous établissements pour comparaison ; - un standard toutes filiales pour synthèse par divisions.

Guide de montage ou de rédaction du rapport d'audit et de relecture par l'audit

- Guide de rédaction du résumé du rapport.
- Support de présentations lors du compte rendu final sur site.

LE COMPTE RENDU ORAL SUR SITE

Le compte rendu oral sur site est une présentation des observations les plus importantes, faite par le chef de mission au principal responsable de l'entité auditée. Il est effectué à la fin du travail de terrain.

Avant de quitter le terrain, l'équipe d'audit doit répondre au souhait légitime, exprimé ou non, du principal responsable de l'entité auditée, d'être informé rapidement et le premier. Ne pas le faire ou refuser de le faire sous prétexte que l'on veut encore réfléchir et/ou prendre du recul serait un aveu d'incompétence. Le faire sans avoir pris ce recul serait de l'imprudence ! L'ossature du rapport, préalablement établie, permet de « débriefing » le principal responsable de l'entité auditée avant de quitter le site pour élaborer le rapport.

Attention : des questions et contestations peuvent naître au cours de cet entretien, nécessitant quelques travaux complémentaires. Ne pas le programmer juste avant de prendre l'avion pour rentrer !

FICHE PRATIQUE

Compte rendu oral sur site

Souhait du principal responsable d'être informé, rapidement, le premier

- Légitime : c'est constitutif d'être responsable.
- Exprimé ou non... et d'autant plus fort que non exprimé !

Y répondre dans l'ossature du rapport

- Quitter sans compte rendu structuré = incompétence.
- Conclure sans prendre de recul = imprudence.

Trucs et astuces

- Synthèse (OR) avant dernières (et secondaires) vérifications.
- CR provisoires (multisites) = observations provisoires, pas conclusions/problèmes.
- Toute l'équipe (explication) et tous les audités (compréhension et engagement), ou informel (déjeuner).
- En profiter pour tester l'acceptabilité des propositions et inciter à la mise en œuvre avant sortie du rapport.

ATTENTION

Des questions et des contestations peuvent entraîner des travaux complémentaires.

C'est le dernier moment informel de travail en commun. Ensuite la relation sera plus formelle (tout en restant cordiale).

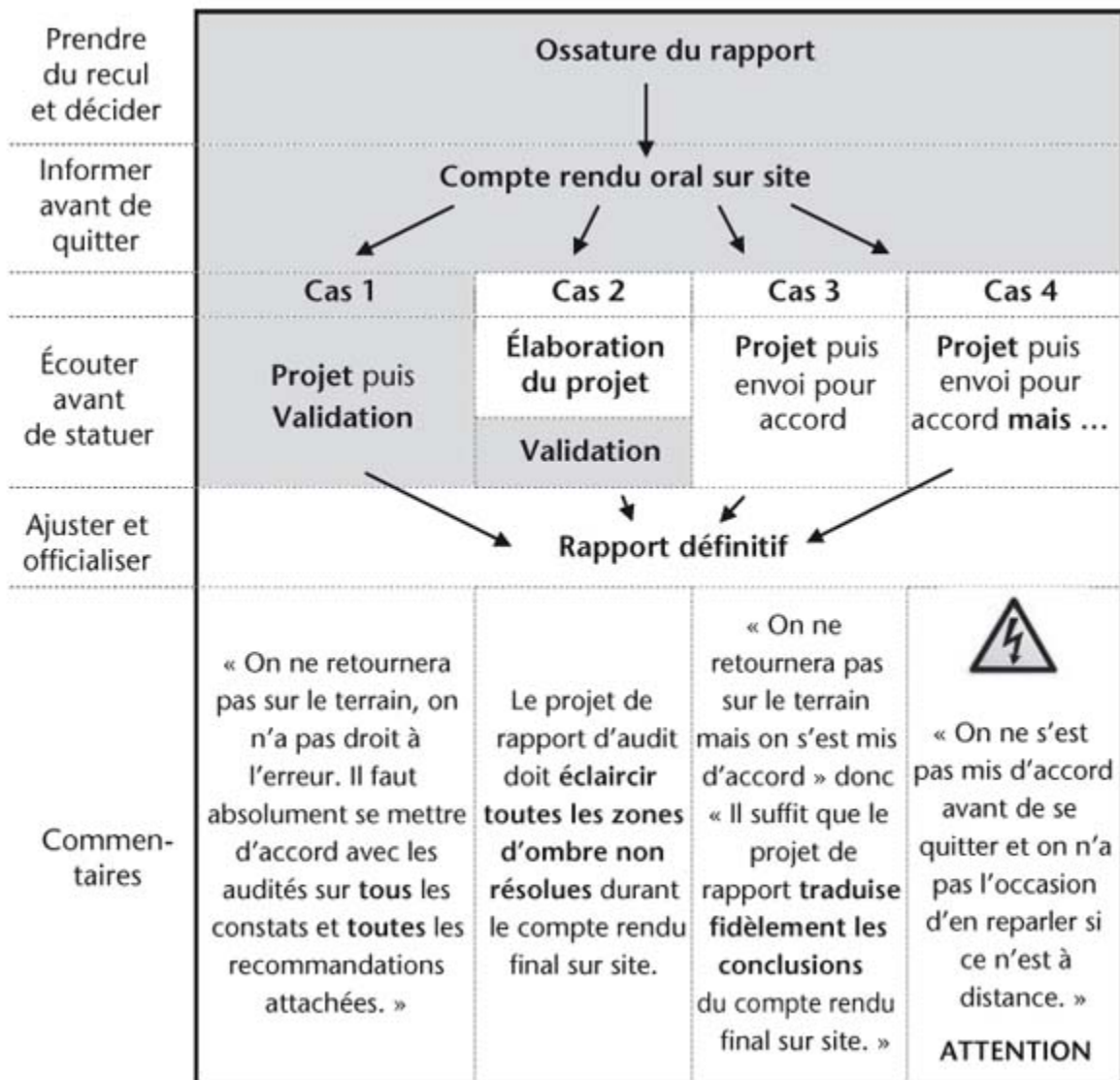
En fonction de l'éloignement entre l'entité auditée et le bureau des auditeurs, plusieurs enchaînements sont envisageables pour cette phase de conclusion de la mission.

- **Cas n° 1** : de par l'éloignement de l'entité auditée, un retour sur le terrain pour la réunion de validation n'est pas possible (coût et temps de transport prohibitifs). La validation finale des conclusions se fait avant de quitter l'entité simultanément au compte rendu final sur site.
- **Cas n° 2** : un retour sur le terrain pour la réunion de validation est possible et nécessaire car le compte rendu final sur site n'a pas permis de dissiper toutes les zones d'ombre, ambiguïtés, litiges entre auditeurs et audités. Les auditeurs rentrent au bureau pour élaborer le projet de rapport d'audit et retournent sur le terrain pour la réunion de validation.
- **Cas n° 3** : un retour sur le terrain pour validation n'est pas nécessaire car durant le compte rendu final sur site, auditeurs et

audités ont balayé tous les points de conclusion de la mission avec validation de chacun d’eux. Les auditeurs élaborent leur projet de rapport d’audit et l’envoient aux audités pour accord.

- **Cas n° 4** : un retour sur le terrain pour validation n’est pas possible mais serait nécessaire car le compte rendu final sur site n’a pas permis de dissiper toutes les zones d’ombre, ambiguïtés, litiges entre auditeurs et audités.

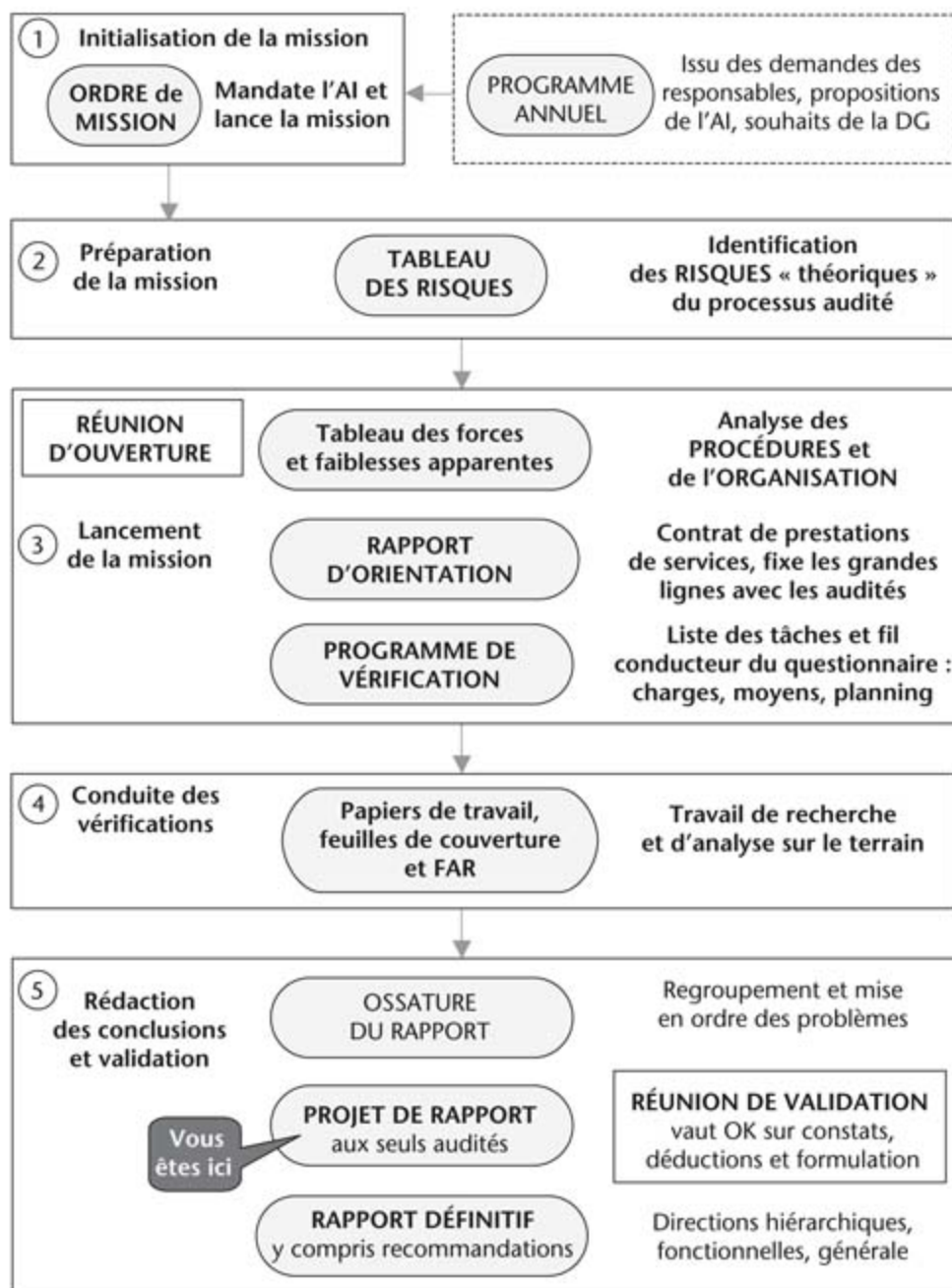
Figure 6.4 – Phases de conclusion d’une mission d’audit interne



(Les phases grisées se déroulent sur le terrain)

Chacune de ces situations est à considérer avec précaution car susceptible de provoquer malentendus, agacements, voire conflits entre auditeurs et audités.

LE RAPPORT D'AUDIT ET SA VALIDATION



Le rapport d'audit interne communique aux principaux responsables concernés pour action, et à la direction pour information, les conclusions de l'audit concernant la capacité de l'organisation auditée à accomplir sa mission, en mettant l'accent sur les dysfonctionnements pour que soient développées des actions de progrès. Il constitue le point culminant de la mission, mais non sa fin.

Le projet de rapport d'audit

À la fin de chaque mission, l'audit rédige un « projet de rapport » formalisant ses constats et recommandations.

Le soin apporté à la relation des faits constatés, à l'analyse de leurs causes et de leurs conséquences, ainsi qu'à la rédaction des recommandations est d'une grande importance : les remarques qui figurent dans un rapport s'adressent à des personnes totalement engagées dans des activités opérationnelles et qui attendent de l'auditeur une parfaite objectivité.

Le projet de rapport constitue un relevé des lacunes, des faiblesses et des dysfonctionnements constatés au cours de la mission, évalués et hiérarchisés en fonction du degré de gravité des conséquences qu'ils induisent. Ce niveau de gravité est mesuré à partir d'éléments factuels chiffrés, recueillis lors des tests réalisés au cours des investigations ; à défaut, la gravité peut être estimée en fonction des enjeux sur lesquels portent les faiblesses et qui ont été identifiés et quantifiés pendant la phase d'étude.

Il est pour les responsables l'occasion de remettre en cause les méthodes de gestion de leurs domaines d'activités ; il n'établit pas un bilan d'une gestion car ce jugement est du ressort de la hiérarchie.

Il reprend la forme des fiches rédigées à la fin de la phase de vérification et comporte à la suite de l'exposition des problèmes (constats, causes et conséquences) un certain nombre de recommandations à l'attention des responsables capables de les prendre en charge, qu'ils soient à l'intérieur ou à l'extérieur de l'entité ou de la fonction auditée. L'importance des recommandations, proportionnelle au degré de gravité des conséquences des dysfonctionnements constatés ou à la signification des enjeux, permet de les classer en recommandations majeures. On entend par recommandations « majeures », les recommandations qui font l'objet d'un suivi particulier par la direction de l'audit.

Le projet de rapport est diffusé aux responsables concernés par le champ de l'audit, dans les meilleurs délais leur permettant d'en prendre connaissance avant la réunion de validation.

La réunion de validation

Une réunion de validation est tenue entre audités et auditeurs, et si nécessaire en présence du commanditaire. Elle a pour objet de recueillir l'avis des audités sur les constats, raisonnements et conclusions de façon à rendre le rapport incontestable.

Il est prévu en introduction à cette réunion de rappeler les objectifs couverts par l'audit, les personnes rencontrées et sites audités, puis d'identifier pour information les points jugés sous contrôle relevés à l'issue de l'analyse des risques ou à l'issue des travaux de vérification. Ces points « forts » seront soulignés dans la note de synthèse présente au sein du rapport définitif.

Dans le cas exceptionnel de désaccord persistant sur la formulation d'un problème ou la pertinence d'une recommandation, les commentaires écrits des responsables audités confirmés par leur hiérarchie sont annexés au cahier des recommandations.

Les recommandations majeures sont confirmées et validées, le délai de leur mise en œuvre est proposé. Les destinataires de ces recommandations sont désignés et chargés de fournir le plan d'actions détaillé.

La réunion de validation vaut accord pour le rapport définitif. La position des audités est enregistrée. Au terme de la réunion de validation, il n'y a plus lieu de commenter mais d'agir.

FICHE PRATIQUE

La réunion de validation

BUT : rendre le rapport non contestable (constats, raisonnements, conclusions, formulation)

- La dernière chance de convaincre et le moment pour obtenir les plans d'actions (norme 2410 : la communication doit inclure les objectifs et le champ de la mission, ainsi que les conclusions, recommandations et plans d'actions).
- Convenir d'un destinataire pour chaque recommandation, jusque-là solution sans pilote.

L'organiser : participants, rôles, diffusion, référencement

La ralentir et la solenniser :

- 1) valider techniquement, page par page, FAR par FAR, le corps du rapport ;
- 2) le responsable de l'audit interne « canalise » le directeur des audités.

En cas de désaccord persistant :

- | |
|--|
| <ol style="list-style-type: none">1) maintenir son opinion : indépendance ;2) mentionner dans le rapport (et insérer le texte de l'audité, approuvé par sa hiérarchie) : objectivité. |
|--|

Rapport définitif

Le rapport définitif se compose d'une part d'une synthèse de trois pages maximum destinée à être lue par les dirigeants, et d'autre part des fiches examinées lors de la réunion de validation et d'une liste des recommandations classées par destinataire précisant la position des audités et constituant de fait leur première réponse à l'audit.

Il est envoyé aux responsables audités en charge de mettre en œuvre les plans d'actions, aux chefs de branche, à leur référent membre du comité exécutif ainsi qu'au président. Il est à noter que le commanditaire initial de la mission fait également nécessairement partie de cette liste de destinataires.

Le rapport d'audit matérialise le travail des auditeurs. Il est recommandé à ses destinataires de ne pas étendre sa diffusion car il contient des informations confidentielles et son style peut surprendre un lecteur non averti.

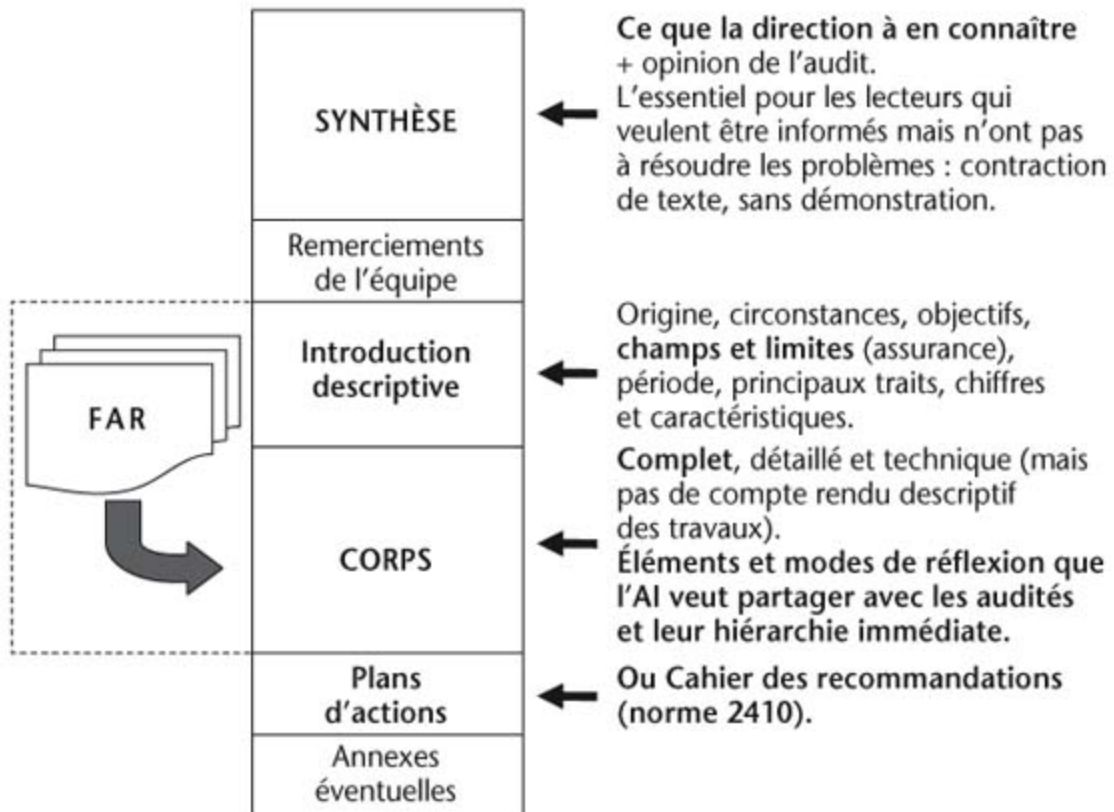
Un rapport d'audit n'est pas neutre : il analyse une situation, mais met prioritairement l'accent sur les dysfonctionnements, pour faire développer des actions de progrès, sans omettre d'évoquer les points forts.

Il contient des recommandations. Une recommandation n'est pas une critique, elle n'implique pas de faute : c'est une amélioration proposée au responsable habilité à mener l'action. Il est en charge de développer et mettre en place une solution au problème soulevé : celle qui a été proposée ou une meilleure.

Après lecture, le président peut inscrire l'examen du rapport à l'ordre du jour d'un comité exécutif ou d'une réunion thématique avec, dans ce cas, la présence des responsables audités et des auditeurs.

Seuls le commanditaire et le président peuvent décider d'une diffusion plus large du rapport. Le président est la seule personne à pouvoir autoriser la communication d'un rapport d'audit à l'extérieur de l'entreprise. Toute demande dans ce sens doit donc lui être soumise.

Figure 6.5 – Le rapport d’audit interne



FICHE PRATIQUE

Le rapport d’audit écrit

Critères de rédaction

- **OBJECTIF** : basé sur des faits, impartial et hiérarchisé (mise en perspective).
- **CLAIR** : aisément compréhensible, logique, langage simple, étayé par suffisamment d'informations.
- **CONCIS** (court ?) : qui va droit au fait, évite les détails. Le minimum de mots possible.
- **UTILE** : constructif, aidant à la réflexion, riche en améliorations... et émis dans un délai permettant d'agir efficacement.

Comité de lecture

Aucun rédacteur ne peut être son propre relecteur : effet produit = effet désiré ?

Présentation

Standardiser pour aider les lecteurs et renforcer l'image de l'audit interne.

Diffusion

Réfléchie et restreinte, parfois partielle.

Prévenir en début de rapport (ou dans une note d'accompagnement) que c'est un rapport d'audit interne.

Focus

Le rapport d'audit

Le rapport d'audit communique aux principaux responsables concernés pour action, et à la direction pour information, les conclusions de l'audit concernant la capacité de l'organisation auditée à accomplir sa mission, en mettant l'accent sur les dysfonctionnements pour que soient développées des actions de progrès. La réunion de validation a pour but de rendre indiscutable le rapport définitif, tant sur le fond que sur la forme. Il constitue le point culminant de la mission, mais non sa fin.

Retour d'expérience

Projet de rapport, réunion de validation et rapport définitif sont les trois temps que l'on retrouve régulièrement dans cette étape méthodologique. Les différences portent principalement sur l'introduction d'un plan d'actions en amont à la diffusion du rapport ou à sa production *a posteriori*.

On notera par ailleurs que de nombreux services d'audit hiérarchisent dans le rapport les recommandations sur plusieurs niveaux en regard de l'importance, des enjeux et de l'urgence dans leurs mises en oeuvre.

Les auditeurs ne participent pas nécessairement à la réunion de validation, laissant à un manager de l'audit le rôle de conduire cette réunion.

La forme et la taille des rapports se réduisent pour privilégier la synthèse plutôt que le contenu détaillé. De ce fait, la vigilance s'impose pour éviter les contestations des audités.

LE SUIVI DES RECOMMANDATIONS

Les destinataires des recommandations majeures identifiés dans le rapport d'audit (désignés en séance de validation) doivent proposer en contrepartie un plan d'actions avec un responsable désigné et une date cible de mise en oeuvre. Ce plan d'actions est annexé au rapport.

Suivi des recommandations (< 3 mois après diffusion du rapport d'audit)

À l'émission du rapport définitif, le chef de mission adresse aux destinataires des recommandations un exemplaire du plan d'actions (cahier des recommandations les concernant), sous forme de fichier informatique chiffré pour raison de sécurité et par messagerie pour faciliter les échanges.

Dans un délai inférieur à 3 mois à compter de la date de réception du rapport, les responsables chargés d'élaborer un plan d'actions doivent répondre directement à la direction de l'audit afin de limiter la discussion aux seules personnes informées des faits détaillés.

Les réponses doivent décrire le plan d'actions qui sera développé pour mettre en place les solutions qui résolvent les problèmes. Elles sont formalisées en complétant le cahier des recommandations qui a été adressé *via* fichier informatique et doivent spécifier les responsabilités et dates de mise en place (maximum 1 an sauf exception) et inclure en annexe les documents nécessaires (notes, procédures...).

Certaines solutions peuvent nécessiter l'intervention d'une ou plusieurs autres fonctions. Il appartient alors aux destinataires des recommandations d'établir une réponse coordonnée en liaison avec les responsables des autres fonctions concernées.

L'équipe d'audit doit examiner chaque point du plan d'actions et vérifier qu'il répond bien au problème soulevé. Les destinataires des recommandations qui ont fourni un plan d'actions détaillé se voient adresser en retour par le chef de mission l'état des actions de progrès qui indique, pour chaque recommandation majeure, l'action décidée pour y répondre et l'avis de la direction de l'audit sur sa pertinence.

Fiche de suivi d'une recommandation

Document à retourner complété au service d'audit interne au plus tard le	
Rapport d'audit publié le	
Recommandation (n°, références, texte) <div style="margin-left: 20px;"> Adressée Affirmative Engageant à l'action </div>	
Réponse établie par (nom, fonction, signature) :	
Décision (cochez) : <input type="checkbox"/> réalisée <input type="checkbox"/> retenue <input type="checkbox"/> à l'étude <input type="checkbox"/> refusée	
Dates prévues	DESCRIPTION du PLAN D'ACTION, y compris responsabilités – Si mise à l'étude : raison, objectifs, responsable, date de décision définitive. – Si refus : raison, signature du manager responsable de la décision.
Cochez si votre plan d'action ne se termine pas à cette page	
Acceptation du plan d'action (codification par l'audit interne)	<input type="checkbox"/> Complet ? <input type="checkbox"/> Exhaustif ? <input type="checkbox"/> Permanent ? <input type="checkbox"/> Contrôlé ? <input type="checkbox"/> Qui ? <input type="checkbox"/> Quoi ? <input type="checkbox"/> Quand ?

Suivi et évaluation des plans d'actions (entre 3 et 9 mois après diffusion du rapport d'audit)

En moyenne, entre 3 et 9 mois après la fin de la mission, le chef de mission contacte ou rencontre le(s) responsable(s) audité(s) et se fait communiquer ou présenter l'état d'avancement des plans d'actions proposés en réponse aux recommandations majeures acceptées. Le

tableau des états d'actions de progrès est mis à jour d'après les éléments présentés.

Une communication est réalisée auprès des directions hiérarchiques ou fonctionnelles concernées.

Bilan des actions de progrès (environ 12 mois après diffusion du rapport d'audit)

La direction de l'audit évalue alors la quantité et la qualité des évolutions intervenues et formule un avis motivé sur la prise en compte et l'efficacité des actions de redressement conduites. Cet avis est formalisé sur une fiche de clôture et adressé au responsable audité, puis aux membres du comité exécutif. Ceux-ci décident en retour de la suite à donner : clôture de la mission, programmation d'un nouveau point ultérieur ou demandes d'explications aux responsables avant clôture, post-audit ciblé sur les éléments non résolus dans des domaines à fort enjeu.

FICHE PRATIQUE

La conclusion d'une mission d'audit interne

Un plan d'actions :

- élaboré par les audités ;
- décidé par eux avec leur hiérarchie ;
- communiqué à l'audit interne pour vérification et réaction éventuelle, et dont la mise en œuvre est suivie.

Critères

Il doit être :

- complet (qui + quoi + quand) ;
- exhaustif (non limité aux secteurs examinés) ;
- permanent (non-réapparition des problèmes) ;
- auto-contrôlé (indicateur de réapparition).

Après l'audit, ce sont les audités qui travaillent !

L'ÉTAT DES ACTIONS DE PROGRÈS

Pour effectuer le suivi, le chargé du suivi, en liaison avec la direction de l'audit, complète le tableau des recommandations établi d'après le cahier des recommandations joint au rapport définitif.

L'état des actions de progrès (EAP) dans sa première version est établi sur la base du cahier des recommandations transmis à l'audité sous forme informatisée dans laquelle il communique son plan d'actions. Il fera l'objet d'une actualisation périodique (EAP1, EAP2...).

Les statistiques (nombre de recommandations émises, nombre de recommandations acceptées, nombre de recommandations en place) sont à saisir dans le tableau de reporting ; les taux de recommandations acceptées et de recommandations en place seront calculés automatiquement au moment de la saisie des nombres précités.

Des suivis intermédiaires sont à programmer en intermission. Ceci peut supposer d'exploiter les réponses des audités à distance ou d'intervenir sur place pour apprécier le plan d'actions.

Postérieurement à la réception des plans d'actions, des questionnaires ouverts sont adressés aux prescripteurs de missions et aux responsables audités. Ils s'inscrivent dans une démarche qualité d'amélioration continue du processus d'audit et visent à mesurer l'apport global de la mission d'audit. Ils permettent d'alimenter un retour d'expérience interne.

En général, les critères de mesure de la performance du service d'audit sont, dans l'ordre : les taux de mise en œuvre des recommandations, de réalisation du plan d'audit, d'acceptation des recommandations et le délai moyen de sortie du rapport.

Le suivi de l'impact de l'audit interne

Un des rôles de l'audit interne est d'évaluer et de promouvoir le contrôle interne. Peu d'entreprises mesurent l'amélioration du contrôle

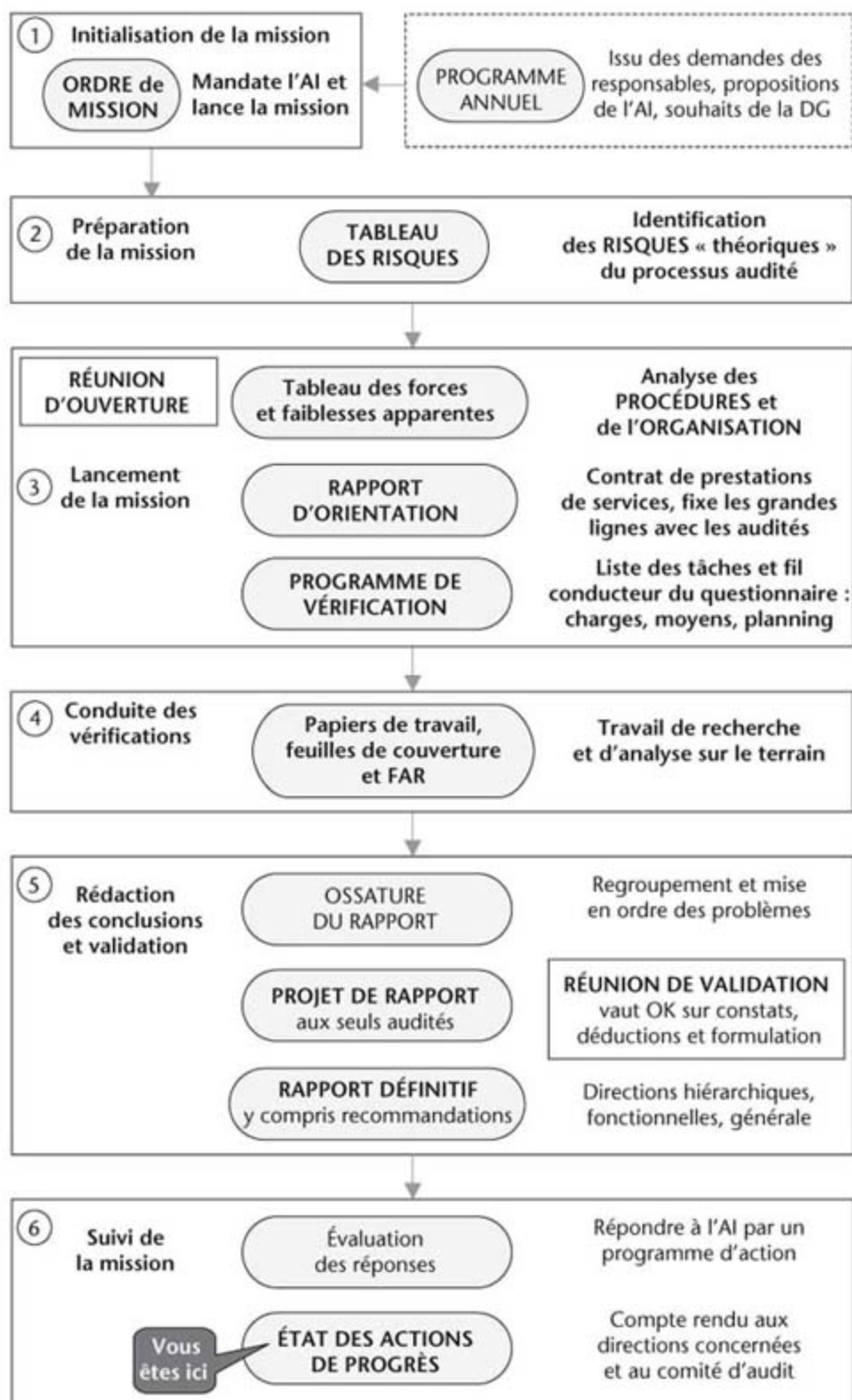
interne due à l'audit interne. « Toutes » suivent le nombre de missions et de rapports, qui est certainement corrélé avec ce rôle, mais il s'agit plus d'un indicateur d'activité que d'impact.

Certains mesurent l'argent que l'audit interne fait gagner. Cela peut être utile – besoin économique de l'entreprise ou politique de l'audit interne (« on s'autofinance ») – et l'on mènera alors des missions sur les constituants du BFR (clients, stocks, fournisseurs ou achats), la gestion de trésorerie ou les taxes (récupération de TVA, taxe professionnelle...). C'est d'ailleurs l'objectif de certaines missions : audit chez un tiers, post-acquisition...

Mais c'est dangereux : l'audit interne est une fonction de prévention, à long terme, par la sensibilisation au contrôle interne, et se servir des gains à court terme pour orienter les missions a un effet pervers. De plus, sommer des réductions de risque et des gains d'efficacité est trompeur.

Si la vocation de l'audit interne est d'impulser des changements, on suivra le taux de mise en œuvre des recommandations, déclarées (reporting) ou vérifiées, à l'issue de la mission ou sous un délai (3 mois et 9 mois).

Quand il est analysé par secteur de l'entreprise, et accompagné du suivi du taux de réponse aux recommandations (ou du délai de réponse), ce suivi met bien en évidence la plus ou moins grande acceptation de l'audit interne. On peut aussi l'analyser par types de recommandations ou de sujets.



Veiller à la mise en œuvre des actions prévues

La réunion de validation et l'obtention des plans d'actions des audités relèvent de la tactique et la demande d'amélioration d'un plan d'actions de la politique : il faut être exigeant sans paraître perfectionniste. Le point suivant relève de la stratégie.

En admettant qu'on ait maintenant un plan d'actions élaboré par les audités, décidé par eux avec leur hiérarchie, et communiqué à l'audit interne pour vérification et réaction éventuelle, qui doit être chargé du suivi de sa mise en œuvre ?

Il est naturel que ce soit l'audit interne : c'est dans le prolongement de sa mission, cela renforce son autorité, et c'est instructif et motivant pour les auditeurs, mais il est plus sage que ce soit la hiérarchie :

- cela reconnaît et renforce pédagogiquement sa responsabilité ;
- cela libère l'audit interne d'une tâche malaisée : les auditeurs sont sur d'autres sujets... quand ils ne sont pas partis du service !

Pour atteindre son objectif – que cela marche mieux après moi qu'avant – le responsable de l'audit interne stratège fera en sorte que la hiérarchie suive et pousse les améliorations, et l'en tienne informé afin qu'il puisse réagir s'il le juge nécessaire. Et il considérera que cette information est comme toutes celles que véhicule le reporting : proche de la vérité, peut-être optimiste.

Focus

L'état des actions de progrès (EAP)

L'EAP permet à l'audit d'obtenir les plans d'actions des audités, de les évaluer et d'assurer la direction que le problème cessera quand les actions seront en place (ou l'alerter), suivre leur mise en place, directement ou indirectement.

Retour d'expérience

Les services d'audit proposent des approches très différenciées quant au suivi des recommandations. Certains services privilégient des audits de suivi sur le terrain après quelques mois, d'autres le font à distance *via* des outils bureautiques, ou le délèguent à des auditeurs dédiés au suivi, voire à d'autres services (contrôle interne, contrôle de gestion).

L'Essentiel

La définition de l'audit interne parle d'une « approche systématique et méthodique ».

L'auditeur interne a besoin de suivre une méthodologie d'investigation précise et détaillée. Elle présente un découpage logique d'étapes débouchant sur des produits.

Du respect scrupuleux d'une méthodologie formalisée dépendent la qualité des missions d'audit réalisées et donc la légitimité de l'activité d'audit.

Pour en savoir plus et approfondir, rendez-vous sur le site : <http://www.audit-interne-referentiels-risques.com>

Chapitre 7

Les documents associés (DA)

EXECUTIVE SUMMARY

- Les documents utilisés par l'auditeur jalonnent le déroulement d'une mission. Ils sont bien évidemment proposés ici à titre d'exemple et devront être adaptés en fonction des spécificités de l'activité d'audit interne concernée (taille du service, pratiques existantes...). Ils sont conçus suivant la chronologie de déroulement de la mission d'audit présentée au chapitre 6.
- Les documents doivent être structurés suivant des modèles types utilisables pour toute mission d'audit. La modélisation de maquettes via l'outil bureautique ou des solutions informatisées permet un gain de temps considérable dans la production de l'auditeur.

ORDRE DE MISSION

L'ordre de mission (OM) est le mandat donné par la direction générale à l'audit interne pour informer les responsables concernés de l'intervention imminente des auditeurs et donner le droit d'accès.

Demandeur	Selon plan d'audit
Type d'audit	Selon plan d'audit
Interlocuteur	Nom du chef de mission
Objet	Intitulé de l'ordre de mission
Date	Le :
Destinataires de l'ordre de mission	
Responsable audité 1	
Responsable audité 2	
Responsable audité 3	
Demandeur	
Copie hiérarchie des audités	
<p>Conformément au plan d'audit de l'année 20XX/20XX, validé par la direction générale, le service de l'audit interne a été mandaté de l'audit de/du (Nom société ou département...).</p> <p>Les objectifs généraux de cette mission sont :</p> <p>Objectif 1).</p> <p>Objectif 2).</p> <p>Objectif N).</p> <p>La mission se déroulera du ... au ..., avec une période d'intervention sur le terrain prévue pour les semaines du ... au ...</p> <p>M. XXX, chef de mission, prendra contact prochainement auprès de vous et de vos principaux collaborateurs que nous vous prions d'informer.</p> <p>Toute l'équipe d'audit et moi-même vous remercions par avance de votre concours actif au bon déroulement de cet audit.</p> <p>M. XXX, pour la direction générale, M. XXX, responsable de l'audit.</p>	

TABLEAU DES RISQUES

Le tableau des risques (TaRi) organise la phase d'étude et conduit à l'élaboration du rapport d'orientation.

AUDIT DE LA FONCTION XXX
<p>Le TaRi associe à une prise de connaissance du domaine à auditer défini par l'ordre de mission, une prise de conscience de ses habituels risques et opportunités d'amélioration, par une décomposition du sujet de la mission en objets auditables.</p> <p>Il produit en première approche le référentiel d'audit.</p> <p>Il permet à l'auditeur de mener une analyse des risques en s'appuyant sur des éléments d'appréciation identifiés par l'audit lors de la phase d'étude, puis d'orienter les travaux détaillés de vérification.</p>
<p>Mission assurée par :</p> <p>Mission supervisée par :</p>

Audit de	Tableau des risques – Référentiel			
Finalités <i>Objectifs de CI :</i> « être sûr que »	Scénarios d'empêchements <i>Risques que les finalités ne soient pas atteintes (que peut-il se passer ?)</i>	Points de contrôle <i>Étapes clés du CI, observables</i> EeADS	Impacts/conséquences <i>Risques si étape clé défaillante/déficiente</i>	Bonnes pratiques Moyens du CI, ressources AaDP
« Être sûr que telle finalité de l'entreprise sera atteinte, que tel aspect/étape du processus audité est sous contrôle, maîtrisé. »	Scénarios de risques : que peut-il se passer ?	Points de passage obligés, concrets, observables : objets à contrôler : • exhaustivité • exactitude • autorisation • délai • suivi/effet attendu	Poids des conséquences : • ¥ € \$ • image, éthique...	Critères de satisfaction – objets auditaibles : • adoptés • adaptés • disponibles • performants
	Qu'est-ce qui peut empêcher d'atteindre la finalité ? Et non : quelles conséquences si elle n'est pas atteinte ?	Qu'est-ce que l'auditeur va contrôler et vérifier en termes d'exhaustivité, exactitude, autorisation, respect des délais... (critères de résultats) ?		Quels moyens et méthodes auraient dû être mis en œuvre par l'audité pour que les résultats soient satisfaisants (= satisfont les critères EeADS) ?

RAPPORT D'ORIENTATION

Le rapport d'orientation définit et formalise les axes d'investigation de la mission et ses limites : il les exprime en objectifs à atteindre par l'audit pour le demandeur et les audités.

AUDIT DE :
Mission assurée par : Chef de mission : Auditeur 1 : Auditeur 2 :

Auditeur 3 :

Auditeur 4 :

Mission supervisée par :

RAPPEL DES OBJECTIFS GÉNÉRAUX DE LA MISSION

- Préoccupations du demandeur, objectifs à atteindre
- Bénéfices attendus des recommandations de l’audit
- Préoccupation des principaux responsables audités

ÉLÉMENTS IDENTIFIÉS LORS DE LA PHASE D’ÉTUDE

- Données chiffrées et évolution

Volumes et types de transactions traitées et chiffres clés. (Résumé)

- Caractéristiques

Caractéristiques propres à l’organisation (Résumé)

AXE DE TRAVAIL ET D’INVESTIGATIONS DE L’AUDIT

- Limites ou exclusions éventuelles du champ de l’audit
- Description des objectifs d’audit (voir tableau ci-après)

AUDIT DE :	Rapport d'orientation	Rédacteur :
Objectifs d'audit retenus Critères de maîtrise du domaine ou de l'activité	Analyse des risques : forces ou faiblesses apparentes en cas de non-atteinte de l'objectif de contrôle	
Premier thème : Premier objectif Second objectif N ^{ème} objectif		
Deuxième thème : Premier objectif Second objectif N ^{ème} objectif		
Troisième thème : Premier objectif Second objectif N ^{ème} objectif		
Quatrième thème : Premier objectif Second objectif N ^{ème} objectif		

PROGRAMME DE VÉRIFICATION

Le programme de vérification est la « gamme de fabrication » à mettre en œuvre pour atteindre les objectifs du rapport d'orientation.

C'est un document interne au service d'audit interne, destiné à définir, répartir, planifier et suivre les travaux des auditeurs par le biais des feuilles de couverture.

AUDIT DE :
Mission assurée par : Chef de mission : Auditeur 1 : Auditeur 2 : Auditeur 3 : Auditeur 4 :
Mission supervisée par :

AUDIT DE :	Programme de vérification	Rédacteur :
-------------------	----------------------------------	--------------------

Le programme de vérification permet au chef de mission de répartir les tâches rattachées à chaque objectif du rapport d'orientation entre chaque auditeur durant une mission. Ce document peut être modifié en cours de mission.

Détails du programme de vérification	Date début	Date fin	Auditeur	Réf. PdT
Objectif 1 (cf. Objectif 1 du rapport d'orientation)				
Tâche 1 : [décrire]				
Tâche 2 :				
Tâche 3 :				
Tâche 4 :				
Tâche 5 :				
Objectif 2 (cf. Objectif 2 du rapport d'orientation)				
Tâche 1 :				
Tâche 2 :				
Tâche 3 :				
Tâche 4 :				
Tâche 5 :				
Objectif 3 (cf. Objectif 3 du rapport d'orientation)				
Tâche 1 :				

BUDGET – PLANNING

Audit de : Sujet / Nom société / Date

	Mois 1															Mois 2															Mois 3																		
	S1					S2					S3					S4					S5					S6					S7					S8					S9					S10			
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5									
Objectif 1																																																	
Tâche 1																																																	
Tâche 2																																																	
Tâche 3																																																	
Tâche n																																																	
Objectif 2																																																	
Tâche 1																																																	
Tâche 2																																																	
Tâche 3																																																	
Tâche n																																																	
Objectif 3																																																	
Tâche 1																																																	
Tâche 2																																																	
Tâche 3																																																	
Tâche n																																																	
Objectif 4																																																	
Tâche 1																																																	
Tâche 2																																																	
Tâche 3																																																	
Tâche n																																																	

FEUILLE DE COUVERTURE DE TEST

La feuille de couverture (FdC) est un document établi en deux temps, avant puis à la fin d'une tâche définie dans le programme de vérification. Elle spécifie les modalités de mise en œuvre puis met en évidence les résultats obtenus.


Feuille de couverture de test	Réf :	Page : ... / ...
Objectif N° 00 Tâche N° aa	Date :	
	Auditeur :	
<ul style="list-style-type: none">• Objectifs du test• Modalités d'exécution• Résultats• Conclusions	Réf. / Commentaires	
	Réf. N° FAR	

FEUILLE DE COUVERTURE D'ENTRETIEN

AUDIT N°	Fiche d'audit et de recommandations	Référence
N° (chapitre) TITRE (du problème) : <i>[Une phrase énonçant de manière synthétique, autonome et percutante les constats, leurs causes et les conséquences]</i>		
Constats : Causes : Conséquences :		
Recommandation : N° (de la recommandation) : Le responsable (préciser fonction) devrait : <i>[action (verbe à l'infinitif)]</i>		
Établie par : Date	Revue par : Date	Soumise à avis de l'audité : Date

PROJET DE RAPPORT D'AUDIT

Le rapport d’audit communique aux principaux responsables concernés pour action et à la direction pour information les conclusions de l’audit.

	Destinataires : voir liste <i>in fine</i>
NOS RÉF. : INTERLOCUTEUR : OBJET :	AAAA/NN – RA Nom du chef de mission  Rapport d’audit – projet <i>[Précisez l’intitulé de la mission]</i> Date :
<p>Veuillez trouver, ci-joint, notre projet de rapport d’audit de (titre).</p> <p>La mission d’audit supervisée par M. S. VISEUR a été effectuée par M. Ch. DEMISS, chef de mission, et M^{mes} A. TRICE et O. DITOSSI, auditeurs. Ce rapport sera discuté lors de la réunion de validation programmée le JJ/MM/20XX.</p> <p>L’objectif de cette réunion de travail est le suivant :</p> <ul style="list-style-type: none">• rendre le rapport non contestable au niveau des constats, raisonnements, conclusions, formulations ;• convenir d’un destinataire pour chaque recommandation, présentée dans le projet comme une proposition d’amélioration ;• évoquer la note de synthèse qui viendra en tête du rapport définitif, dont l’objet est destiné aux lecteurs qui doivent être informés mais n’ont pas à résoudre les problèmes. <p>Après validation des constats et recommandations, le rapport sera diffusé conformément au processus de fin d’audit décrit.</p> <p>Prénom NOM <i>Le directeur de l’audit</i></p> <p><i>Copie :</i></p>	

RAPPORT D’AUDIT

	Destinataires : voir liste <i>in fine</i>
NOSRÉF. : INTERLOCUTEUR : OBJET :	AAAA/NN – RA Nom du Responsable de l'audit  Rapport d'audit <i>[Précisez l'intitulé de la mission]</i> Date :
<p>Veuillez trouver, ci-joint, le rapport d'audit de (titre).</p> <p>La mission d'audit supervisée par M. S. VISEUR a été effectuée par M. Ch. DEMISS, chef de mission, et M^{mes} A. TRICE et O. DITOSSI, auditeurs.</p> <p>Les constats et recommandations développés dans ce rapport ont été validés lors d'une réunion effectuée le JJ/MM/20xx.</p> <p>Le rapport se présente sous forme d'une note de synthèse (de couleur bleue) suivie d'une liste de fiches détaillant les résultats de l'audit, puis d'un cahier des recommandations (en vert).</p> <p>Conformément au processus rappelé en annexe du rapport, le ... <i>[indiquez le titre et la fonction de la personne chargée de coordonner les réponses au cahier des recommandations]</i> adressera son plan d'actions à la direction de l'audit, au plus tard pour le JJ/MM/20XX.</p> <p>Prénom NOM <i>Le directeur de l'audit</i></p> <p><i>Copie :</i></p>	

Date d'envoi	RAPPORT D'AUDIT TITRE DE LA MISSION PÉRIODE D'INTERVENTION :
<p>Ce document est un rapport d'audit qui matérialise le travail des auditeurs effectué dans le cadre d'une mission.</p> <p>Il est vivement recommandé à ses destinataires de ne pas étendre sa diffusion car :</p> <ul style="list-style-type: none"> – il contient des informations confidentielles ; – son style peut surprendre un lecteur non averti. <p>Ce rapport analyse une situation et met en évidence des dysfonctionnements de l'organisation, en vue de développer des actions de progrès.</p> <p>Les recommandations consistent à proposer la mise en place d'une amélioration au responsable habilité à mener l'action en vue de résoudre un problème.</p> <p style="text-align: center;"> Document strictement interne à diffusion restreinte Communication externe interdite Reproduction soumise à autorisation </p>	

Équipe d'audit

Directeur de l'audit :	Nom Prénom
Chef de mission :	Nom Prénom
Auditeurs :	Nom Prénom, Nom Prénom, Nom Prénom
Chargé du suivi post-audit à la direction de l'audit :	Nom Prénom

Réunion de validation

Date	Participants		
	Nom	Prénom	Fonction

Rédaction – validation

Chef de mission		Responsable de l'audit		Responsable des audités	
Date	Visa	Date	Visa	Date	Visa

Diffusion

Destinataires de l'original			Destinataires de copie		
Nom Prénom (responsable de l'élaboration du plan d'actions)	Fonction	Nb	Nom Prénom	Fonction	Nb

SOMMAIRE

1. SYNTHÈSE

2. INTRODUCTION DESCRIPTIVE

A) Champ de l'audit

B) Déroulement de la mission

C) Rappel des objectifs de la mission

D) Éléments identifiés lors de la phase d'étude

3. FICHES D'AUDIT ET DE RECOMMANDATIONS

N° 1 – Titre

N° 2 – Titre

N° 3 – Titre

4. SYNTHÈSE ET HIÉRARCHISATION DES RECOMMANDATIONS

5. SUIVI DES RECOMMANDATIONS / PLAN D'ACTIONS

6. ANNEXES

1. SYNTHÈSE

2. INTRODUCTION DESCRIPTIVE

A) *Champ de l'audit*

Durant la période de *JJ Mois Année* à *JJ Mois Année*, nous avons effectué un audit interne à l'entité *X, Localisation, Région*. Un plan d'actions concernant la mise en recommandations est joint en annexe au présent rapport.

Notre audit inclut les processus suivants :

• Xxx	• Xxx
• Xxx	• Xxx
• Xxx	• Xxx
• Xxx	• Xxx

B) *Déroulement de la mission*

C) Rappel des objectifs de la mission

D) Éléments identifiés lors de la phase d'étude

3. FICHES D'AUDIT ET DE RECOMMANDATIONS

N° 1 – Titre

Constat :

Cause :

Conséquences :

Recommandations :

Le (*fonction*) doit (ou devra) : ...

4. SYNTHÈSE ET HIÉRARCHISATION DES RECOMMANDATIONS

Ce chapitre doit présenter, dans une forme visuelle appropriée, l'ensemble des recommandations hiérarchisées.

Le (*fonction*) doit (ou devra) :

R 1

R 2

R 3

R n

5. SUIVI DES RECOMMANDATIONS / PLAN D' ACTIONS

R 1

Recommandation	réalisée <input type="checkbox"/>	retenue <input checked="" type="checkbox"/>	à l'étude <input type="checkbox"/>	refusée <input type="checkbox"/>
Commentaires/ dates prévues :				

R 2

Recommandation	réalisée <input type="checkbox"/>	retenue <input type="checkbox"/>	à l'étude <input checked="" type="checkbox"/>	refusée <input type="checkbox"/>
Commentaires/ dates prévues :				

R 3

Recommandation	réalisée <input checked="" type="checkbox"/>	retenue <input type="checkbox"/>	à l'étude <input type="checkbox"/>	refusée <input type="checkbox"/>
Commentaires/ dates prévues :				

R n

Recommandation	réalisée <input type="checkbox"/>	retenue <input type="checkbox"/>	à l'étude <input type="checkbox"/>	refusée <input checked="" type="checkbox"/>
Commentaires/ dates prévues :				

SUIVI DES RECOMMANDATIONS / PLAN D'ACTIONS

Les destinataires des recommandations majeures identifiés dans le rapport d'audit doivent proposer en contrepartie un plan d'actions avec

un responsable désigné et une date cible de mise en œuvre. Ce plan d'actions est annexé au rapport.

Le (*fonction*) doit (ou devra) :

R1 : en liaison avec (*fonction*) :

Élaborer :

Suite donnée :	<input type="checkbox"/> action réalisée	<input type="checkbox"/> action retenue
	<input type="checkbox"/> action à l'étude	<input type="checkbox"/> action refusée
Réponse établie par (<i>nom, fonction, date</i>) :		
<p>Description du plan d'actions y compris responsabilités et dates prévues : Raison, objectifs, responsabilités, date de décision définitive en cas de mise à l'étude. Raison, engagement du manager assumant les conséquences en cas de refus.</p>		
Avis de la direction de l'audit :		
Avis motivé sur le plan d'actions et éléments probants demandés si souhaités.		

ÉTAT DES ACTIONS DE PROGRÈS

L'état des actions de progrès permet de rendre compte régulièrement des suites données aux recommandations formulées par l'audit et des résultats obtenus par les actions correctives des audités.

Les plans d'actions sont définis par les audités : c'est leur responsabilité. La responsabilité de l'audit interne est d'obtenir ces plans d'actions et d'évaluer s'ils répondent aux problèmes relevés.

Rapport d'audit publié le (*date du rapport définitif*)

ÉTAT DES ACTIONS DE PROGRÈS

Réponses dues le (*préciser la date attendue pour le retour des fiches*)

Suivi au (*date du suivi*)

Mission assurée par :

Chef de mission :

Auditeur 1 :

Auditeur 2 :

Auditeur 3 :

Auditeur 4 :

Mission supervisée par :

Rappel des éléments de recommandations issus du rapport d'audit publié le (JJ/MM/AA)						Suivi du plan d'actions au (JJ/MM/AA)		
Numéro et descriptif de la recommandation	Responsable de la mise en œuvre	Date de réponse des audités	Recommandation acceptée (précision)	Date mise en place prévue	Recommandation refusée (motif évoqué)	Avis de la direction de l'audit sur les actions proposées	Recommandation en place Oui/Non	Date mise en place réalisée
Nombre de recommandations émises =			Nombre de recommandations acceptées = Taux de recommandations acceptées = %				Nombre de recommandations en place = Taux de recommandations en place = %	

FICHE DE CONSEILS DE PERFECTIONNEMENT POST-AUDIT

Fonction : auditeurs	
Renseignement auprès de :	
NOM : Prénoms : Date d'entrée à : Date d'entrée dans la fonction audit : Formation initiale :	
Titre et numéro de la mission d'audit : Période de l'audit : Lieu :	
Caractéristiques des sections d'audit confiées = <i>Légende : Complexe/Normal/Facile</i>	
Rappel des conseils de perfectionnement indiqués lors des précédentes missions :	
<i>Indiquez par un signe l'appréciation portée : ↗ à améliorer → maintenir</i>	
Tête	<ul style="list-style-type: none"> • qualité du travail d'audit : • connaissances techniques : • compréhension des problèmes : • capacité de synthèse : • méthode et sens de l'organisation :
Sécurité	<ul style="list-style-type: none"> • respect des règles et instructions : • fiabilité : • qualité des papiers de travail (clarté, soin, référencement...) :
Sourire	<ul style="list-style-type: none"> • sens de la convivialité : • esprit d'équipe : • attitude professionnelle : • capacité de travail sous pression :
Cœur	<ul style="list-style-type: none"> • adaptabilité : • créativité : • qualité relationnelle : • maturité :
Main	<ul style="list-style-type: none"> • implication personnelle : • prise d'initiative : • sens du management : • capacité de réalisation :
Jambes	<ul style="list-style-type: none"> • dynamisme : • mobilité : • connaissances du groupe :
Principales compétences du collaborateur : – contribuant à le faire apprécier dans sa fonction actuelle : – à développer pour accroître son efficacité :	
Remarques éventuelles de l'intéressé :	
Date de l'entretien : Réaliser par : Transmis au directeur de l'audit le :	

Fonction : chef de mission	
Renseignement auprès de :	
NOM : Prénoms : Date d'entrée à : Date d'entrée dans la fonction audit : Formation initiale :	
Titre et numéro de la mission d'audit : Période de l'audit : Lieu :	
Caractéristiques des sections d'audit confiées = <i>Légende : Complexe/Normal/Facile</i>	
Rappel des conseils de perfectionnement indiqués lors des précédentes missions :	
<i>Indiquez par un signe l'appréciation portée : ↗ à améliorer → maintenir</i>	
Direction	<ul style="list-style-type: none"> • diriger la phase d'étude : • planifier et répartir le travail terrain : • assurer son avancement section par section : • organiser l'achèvement de la mission : • méthode et sens de l'organisation :
Expertise	<ul style="list-style-type: none"> • connaissances et application des techniques d'audit : • connaissances et application des référentiels d'entreprises : • caractère complet et explicite des objectifs, conclusions et explications : • qualité de la synthèse du rapport :
Encadrement	<ul style="list-style-type: none"> • faire appliquer la méthodologie et contrôler la qualité du travail : • garantir le renseignement de la base mission : • animer l'équipe, former et évaluer les auditeurs : • capacité à faire travailler sous pression :
Représentation	<ul style="list-style-type: none"> • aptitude à communiquer les problèmes de façon sélective et rapide : • attitude professionnelle : • capacité de discussion des rapports : • qualité relationnelle : • maturité :
Performances	<ul style="list-style-type: none"> • implication personnelle : • prise d'initiative : • sens du management : • dynamisme :
Principales compétences du collaborateur : – contribuant à le faire apprécier dans sa fonction actuelle : – à développer pour accroître son efficacité :	
Remarques éventuelles de l'intéressé :	
Date de l'entretien : Réalisé par : Transmis au directeur de l'audit le :	

QUESTIONNAIRE DE SATISFACTION POST-AUDIT

AUDIT DE :

OBJECTIF

L'évaluation des missions par les fonctions auditées s'inscrit dans une démarche qualité d'amélioration continue du processus de l'audit :

- entretenir le dialogue avec les audités ;
- mesurer l'apport global de la mission d'audit ;
- améliorer les méthodes d'audit ;
- apprécier le comportement des auditeurs.

DÉLAI

Le questionnaire est adressé après obtention du premier plan d'actions reçu des audités.

Merci de bien vouloir nous faire parvenir vos remarques sous huitaine.

Mission assurée par :

Mission supervisée par :

« Veuillez trouver ci-après un questionnaire d'évaluation de la mission qui s'est déroulée sur votre site pendant ...

Ce questionnaire est à usage interne et s'inscrit dans une démarche qualité d'amélioration continue de la satisfaction des clients de l'audit interne. Nous vous demandons de bien vouloir y répondre en toute objectivité et nous le retourner dans les meilleurs délais. »

Mission N° :		Titre de l'audit :		
Nom :		Fonction :	Date :	

Liste des questions		Oui	Non	Pourquoi – comment ?
	<i>Lancement de la mission</i>			
1	Lettre de mission : avez-vous été informé de la mission dans des délais satisfaisants (sinon quel délai vous semble souhaitable) ?			
2	Les auditeurs vous ont-ils expliqué le rôle et l'activité de la direction de l'audit ?			
3	Vous ont-ils expliqué les objectifs de la mission ?			
4	Aviez-vous formulé des demandes complémentaires qui n'ont pas été prises en compte et si oui, lesquelles ?			
5	Vous ont-ils expliqué comment la mission allait se dérouler, ce qu'ils allaient faire et ce que vous auriez à faire ?			
6	Ces présentations vous ont-elles semblé utiles ?			
	<i>Déroulement de la mission</i>			

Liste des questions		Oui	Non	Pourquoi – comment ?
7	Le déroulement des interviews et des tests vous a-t-il paru satisfaisant (sinon pourquoi) ?			
8	Les auditeurs avaient-ils une bonne connaissance des caractéristiques de votre unité ou de la fonction auditée ?			
9	Les conclusions de la phase d'étude – analyse rapide de votre organisation et de son fonctionnement, détermination des points forts et des points faibles apparents – vous ont-elles été présentées (cf. rapport d'orientation) ?			
10	Les informations recueillies et les vérifications effectuées ont-elles été traitées de manière convaincante ?			
11	Les audités ont-ils été informés en cours de mission des points relevés par les auditeurs ?			
12	Les audités ont-ils pu exprimer leur position et leurs arguments sur les constats des auditeurs ?			
13	Les audités ont-ils été associés à la recherche de solutions ?			
14	La mission s'est-elle déroulée sans trop perturber le fonctionnement des services audités (sinon pourquoi) ?			
15	Avez-vous des suggestions à émettre quant au comportement des auditeurs ?			
	<i>Conclusion de la mission</i>			
16	Avez-vous eu une restitution orale des principaux constats relevés par l'audit, juste avant le départ ?			
17	Avez-vous pu vous prononcer sur le projet de rapport avant l'émission du rapport définitif ?			
18	Vos éventuelles divergences ont-elles été prises en compte dans le rapport définitif (modification ou annotation) ?			
19	Le délai d'émission du projet de rapport est-il satisfaisant (sinon quel délai vous semble-t-il souhaitable) ?			
20	Le délai annoncé d'émission du rapport définitif a-t-il été respecté ?			
21	Les recommandations sont-elles pertinentes (sinon précisez) ?			
22	La forme des rapports vous semble-t-elle efficace (structure, présentation, longueur) ?			
23	La mission vous a-t-elle apporté une meilleure connaissance des pratiques en vigueur dans votre entité ?			

Liste des questions		Oui	Non	Pourquoi – comment ?
24	Une meilleure connaissance des dispositifs de contrôle ?			
25	Vous a-t-elle révélé des problèmes significatifs ?			
26	A-t-elle confirmé des difficultés en les cernant avec suffisamment de précision pour vous permettre d'agir ?			
<p>Commentaires sur l'apport global de la mission d'audit interne :</p> <p>Avez-vous d'autres remarques à faire et propositions à formuler pour les missions futures, chez vous ou ailleurs ?</p> <p>L'équipe d'audit et la direction de l'audit vous remercient de votre participation.</p>				

L'Essentiel

- Ce chapitre reprend d'une manière organisée une série de documents de référence qui permettent la production des produits méthodologiques durant la mission. Il s'agit de bâtir et d'argumenter le dossier pour établir objectivement une conviction.
- Ces documents aident l'auditeur à tracer d'une manière objective et efficace son opinion et ses éléments de preuve. En effet, l'auditeur doit-être à même de justifier chaque point de son rapport, d'apporter la preuve des faits qu'il rapporte et de l'évaluation correcte des impacts qu'il indique.

Partie 3 Les outils de l'audit interne

[Les techniques d'audit traditionnelles \(TA\) Chapitre 8](#)

[Les nouveaux outils liés aux évolutions technologiques Chapitre 9](#)



Chapitre Les techniques d'audit traditionnelles

8 (TA)

EXECUTIVE SUMMARY

■ Une méthode sans outils, c'est insuffisant ! Les éléments essentiels des outils et techniques que l'auditeur peut avoir l'occasion d'utiliser lors de la conduite de sa mission d'audit interne sont présentés d'une manière synthétique et pédagogique dans ce chapitre.

■ Pour chacun de ces outils, on répondra aux questions suivantes : À quoi ça sert ? Quand l'utilise-t-on ? Comment l'utilise-t-on, et qui l'utilise ? Quels sont les avantages, inconvénients et limites de l'outil ?

Parmi les techniques d'audit les plus utilisées et sans que cela constitue une présentation exhaustive, nous avons identifié onze outils à la disposition de l'auditeur.

Il y a lieu de distinguer le recours à ces techniques en regard de l'objectif poursuivi. On distinguera quatre types d'approches.

• Les approches globales :

- analyse économique et financière ;
- volume et types de transactions ;
- diagrammes de circulation (*flow charts*) ;
- grille de séparations des tâches.

• Les approches par questionnaire :

- interviews ;

– questionnaires administrés QCM-QO (à choix multiples ouverts) et questionnaires QCI (de contrôle interne).

• **Les approches par vérifications :**

- piste d’audit (*audit trail*) ;
- observations physiques ;
- rapprochements et reconstitutions ;
- interrogations de fichiers informatiques ;
- sondages statistiques.

• **Les nouveaux outils liés aux évolutions technologiques ([chapitre 9](#)).**

Pour certains outils, une page de commentaires apportera des compléments d’informations et/ou des exemples afin d’en guider la mise en œuvre.

L’analyse économique et financière

À quoi ça sert ?

L’analyse économique et financière est un ensemble de travaux préliminaires d’analyse sur les données chiffrées de la fonction ou entité auditée, qui permet de :

- situer l’entité auditée et comprendre son évolution et son contexte ;
- situer l’importance du sujet demandé par le commanditaire à l’audit (enjeux et rôle stratégique pour l’organisation de tutelle) ;
- situer les ordres de grandeur, connaître les chiffres significatifs, déterminer les seuils de matérialité.

Elle peut permettre de détecter certains risques globaux : ratios financiers et/ou évolutions préoccupantes.

Quand l'utilise-t-on ?

L'analyse économique et financière est une technique utilisée en phase d'étude (initialisation de la mission et examen de l'activité et élaboration d'un référentiel de risques).

Comment l'utilise-t-on et qui l'utilise ?

Pour une entité on se préoccupera plus particulièrement de :

- l'analyse financière sur 3 à 5 ans ;
- l'étude des budgets N et N + 1 ;
- l'analyse des plans de financement et besoins en fonds de roulement ;
- le calcul du taux de rotation des stocks ;
- l'analyse ABC des clients et des fournisseurs ;
- l'analyse de rentabilité.

Pour un processus ou une fonction :

- fonction commerciale ou achats : nombre d'offres (ou de consultations) établies, et/ou ayant fait l'objet d'une commande ;
- gestion de la production : nombre de lancements en fabrication par rapport au nombre de commandes clients, indicateurs de performance et de service ;
- flux administratifs : volume et types de transactions.

Avantages/inconvénients (limites) de l'outil

L'analyse économique et financière permet d'apprécier les enjeux financiers et stratégiques des différents aspects de la thématique auditée (groupe, filiales, agences, usines, processus...). L'auditeur peut ainsi

orienter ses travaux vers les éléments les plus significatifs en accord avec les attentes du demandeur. La nature et le nombre d'indicateurs et de ratios étant inépuisables, l'auditeur doit veiller à ne se préoccuper que de ceux pertinents au regard de la problématique auditée. L'exploitation de ces données est d'autant plus intéressante si elles peuvent être comparées avec les mêmes valeurs d'autres entités semblables (autres filiales du groupe, autres agences...).

Les volumes et types de transactions

À quoi ça sert ?

L'approche par les volumes et types de transactions permet de situer les enjeux du sujet audité par l'analyse de données statistiques (globales, non comptables, exprimées souvent par des quantités et non des valeurs monétaires). Il s'agit par exemple du nombre de commandes fournisseurs, factures clients, articles en stock, transactions informatiques, écritures comptables... Ou encore des ratios : nombre de commandes par personne, taille moyenne d'une commande, nombre d'avoirs par facture... Alors que l'analyse économique et financière quantifie l'entité ou la fonction auditée, l'approche « Volumes et types de transactions » quantifie son organisation. Par exemple, un même chiffre d'affaires peut être réalisé avec « beaucoup de petites commandes » ou avec « un nombre limité de grosses affaires ». Les deux organisations concernées seront très différentes (effectifs, systèmes d'informations...), ainsi que les risques associés. L'audit doit évidemment tenir compte des spécificités organisationnelles du domaine audité.

Quand l'utilise-t-on ?

Comme pour l'analyse économique et financière, l'approche « Volumes et types de transactions » est utilisée en phase d'étude (initialisation de la mission et examen de l'activité et élaboration d'un référentiel de risques).

Comment l'utilise-t-on et qui l'utilise ?

L'auditeur peut utiliser diverses méthodes :

- les comparaisons : chronologiques (évolution d'une donnée au fil du temps), synoptiques (entre entités semblables d'une même organisation ou entre organisations d'un même secteur d'activité) ;
- les corrélations : étude des grandeurs observées qui ont un lien de dépendance logique.

Cette technique d'audit permet à l'auditeur de repérer :

- des variations anormales (soudaines et de forte amplitude) ;
- des différences significatives entre entités et/ou organisations comparées ;
- des évolutions contraires aux tendances observées dans le domaine.

Ces approches ne font que révéler le phénomène, les anomalies constatées devront être explicitées dans la suite de la mission.

Avantages/inconvénients (limites) de l'outil

Les sources d'informations nécessaires aux comparaisons ne sont pas toujours connues et disponibles pour les auditeurs. Par ailleurs, s'agissant principalement des données extracomptables, l'auditeur doit rester prudent et s'assurer de leur fiabilité. Enfin, il est nécessaire de définir des seuils de signification au-delà desquels une évolution sera qualifiée d'anormale.

Les diagrammes de circulation (*flow charts*)

À quoi ça sert ?

Le diagramme de circulation des documents ou *flow chart* est une représentation graphique décrivant la suite des opérations réalisées dans le cadre d'un processus. La nature des tâches et contrôles effectués, les documents et supports utilisés, les outils pratiqués sont représentés par des symboles reliés les uns aux autres pour chaque acteur du processus. Le

diagramme permet de visualiser de manière globale le cheminement des informations, ce qui facilite l'analyse du processus étudié. Son élaboration par les auditeurs permet :

- de mieux cerner la procédure dans ses détails ;
- de donner une vue complète de l'enchaînement des opérations ;
- de vérifier la cohérence, la validité et l'efficacité des dispositifs de contrôle interne ;
- d'en dégager les forces et les faiblesses.

Le diagramme de circulation n'est pas seulement un outil de description mais aussi un outil de pré-analyse. Le diagramme de circulation est un moyen efficace pour connaître et comprendre l'organisation des processus étudiés ainsi que les points de contrôle existants dans le cadre des procédures en vigueur. En matière de démarche d'audit, il permet de mettre plus particulièrement en évidence :

- des lourdeurs administratives dans le traitement de l'information (cheminement complexe des documents, double archivage ou archivage inutile) ;
- des redondances dans les contrôles réalisés (contrôles similaires réalisés par deux services différents) ;
- des concentrations excessives de tâches réalisées au sein d'un même service (non-respect du principe de séparation des fonctions).

Quand l'utilise-t-on ?

L'auditeur utilise cet outil lors de la prise de connaissance du domaine audité (phase de lancement de la mission sur site). À ce niveau de la phase d'étude, schématiser le processus sous forme de diagramme lui permet ainsi de comprendre facilement et rapidement le fonctionnement du processus concerné. Indépendamment d'une mission d'audit interne, cet outil peut aussi être utilisé lors de la formalisation d'une procédure au sein

de l'organisation (qu'il s'agisse de procédures de contrôle interne, de procédures exigées dans le cadre d'un système de management de la qualité conforme aux normes ISO 9001, ou de tout autre système documentaire).

Comment l'utilise-t-on et qui l'utilise ?

L'élaboration d'un diagramme de circulation est essentiellement basée sur l'interview des audités ou sur la base des procédures écrites existantes. Cet outil à la disposition de l'auditeur doit faire ressortir de manière claire et précise :

- la nature des opérations réalisées et les intervenants concernés ;
- les documents utilisés (nombre d'exemplaires, destinataires respectifs).
L'auditeur doit se procurer une copie de chaque document utilisé afin d'illustrer le diagramme de circulation ;
- les modes de classement (archivage physique, support informatique...).

Avantages/inconvénients (limites) de l'outil

L'élaboration d'un diagramme de circulation facilite la découverte du domaine audité. Il permet également de mettre en évidence les faiblesses du contrôle interne. Il constitue par ailleurs un outil de communication pour l'auditeur lors de sa validation par les audités en lui garantissant une bonne compréhension du processus audité. Il peut enfin constituer une valeur ajoutée supplémentaire à la mission d'audit.

Cependant, cette technique d'audit nécessite un minimum de formation et de pratique. Des logiciels dédiés facilitent grandement la mise en œuvre de cet outil.

Des notes complémentaires sont souvent nécessaires à l'appui d'un diagramme de circulation pour expliciter la symbolique utilisée.

Exemples de symbolisation

 Illustration

 Illustration

La grille de séparation des tâches

À quoi ça sert ?

La grille de séparation des tâches permet de comprendre, par rapport à la chronologie des opérations réalisées dans un processus ou une fonction, la répartition des responsabilités entre les différents acteurs à un instant donné. L'auditeur établit cette grille (ou l'exploite si elle existe par ailleurs) afin de s'assurer du respect d'un principe de base du contrôle interne : « la séparation des fonctions ». En effet toute organisation doit veiller à séparer les responsabilités de « détention/manipulation », d'« enregistrement » et d'« approbation/décision » sans quoi elle s'expose à un risque majeur au niveau de ses actifs si des collusions s'instaurent entre les acteurs. Grâce à cette grille, l'auditeur vérifie qu'il n'y a pas cumul de fonctions sur un même acteur ou un groupe restreint d'entre eux. Cet outil met aussi en évidence des éventuelles anomalies concernant la répartition de la charge de travail entre les différents intervenants.

Quand l'utilise-t-on ?

Principalement lors de la phase de conduite des vérifications afin de rechercher les preuves de faiblesses du contrôle interne en la matière.

Comment l'utilise-t-on et qui l'utilise ?

Une grille peut être conçue pour chaque grand processus ou fonction de l'organisation. Dans une première colonne sont listées les différentes tâches du processus concerné. Une deuxième colonne indique la nature de la tâche au regard des grandes catégories de responsabilités en principe inconciliables entre elles. Les colonnes suivantes indiquent les personnes en charge des différentes étapes. L'analyse par colonnes permet de découvrir une personne qui effectue plusieurs tâches et la compatibilité

entre ces différentes tâches. L'analyse par lignes permet de découvrir une tâche effectuée plusieurs fois ou non réalisée. La grille d'analyse des tâches peut également être utilisée par les organisateurs pour mesurer le travail de chacun.

Avantages/inconvénients (limites) de l'outil

La grille d'analyse de tâches est relativement simple à élaborer (en fonction de l'importance du processus étudié et de sa complexité). Elle constitue pour l'auditeur un outil incontournable d'appréciation du principe de séparation des fonctions. Dans la phase de conclusion, l'auditeur peut également l'utiliser pour fonder ses recommandations concernant une meilleure utilisation des moyens humains disponibles. Indépendamment d'une mission d'audit, cet outil peut être généralisé dans le cadre d'une démarche de réorganisation plus globale.

Cependant, la grille d'analyse des tâches a ses limites :

- elle reflète une situation organisationnelle à un instant donné (aspect statique de l'outil) ;
- lorsqu'elle a été établie à la suite d'interviews avec les audités, il est nécessaire de vérifier sur le « terrain » qu'elle correspond effectivement à la réalité ;
- le principe de séparation des fonctions doit être appréhendé en tenant compte des contraintes liées aux effectifs disponibles dans les services concernés (notamment dans les organisations de taille modeste). Une recommandation d'audit qui conduirait à un doublement des effectifs afin de respecter scrupuleusement ce principe constituerait probablement une aberration. Dans ce cas de figure, d'autres dispositifs de contrôle interne sont envisageables (exemple : renforcement de la supervision).

Exemples de grille de séparation des tâches

Processus : ACHATS

 Illustration

 Illustration

Processus : VENTES

 Illustration

 Illustration

Processus : GESTION DES STOCKS

 Illustration

Processus : PAIE

 Illustration

Les interviews

À quoi ça sert ?

L'interview est plus qu'un entretien, elle permet à l'auditeur d'appréhender les différents processus de l'organisation en posant des questions aux personnes impliquées dans le domaine audité. Il peut ainsi recueillir de l'information afin de comprendre, pour chaque opération réalisée : les objectifs poursuivis, la nature des tâches exécutées, les documents utilisés, les difficultés rencontrées et ainsi identifier les risques potentiels.

L'interview apportera une plus-value à la collecte des informations factuelles en termes d'éléments d'analyse et de jugement et pourra aussi servir dans certains cas pour délimiter le champ et les objectifs.

Quand l'utilise-t-on ?

Éventuellement lors de la phase d'initialisation de la mission d'audit afin d'établir le projet d'ordre de mission : il s'agit de se faire préciser, si

nécessaire, dans le cadre d'entretiens avec les commanditaires, leurs attentes et préoccupations particulières. Lors de la phase de lancement de la mission sur site afin de comprendre le domaine audité et d'identifier les faiblesses potentielles de contrôle interne.

Comment l'utilise-t-on et qui l'utilise ?

Une interview : avant « ça se prépare », pendant « ça se maîtrise », après « ça s'exploite ». En complément du guide on retiendra les points essentiels suivants.

Avant

Préparer sa thématique en établissant un guide ou canevas d'entretien (thèmes à aborder, documents à récupérer, points à détailler au regard des préoccupations du commanditaire de la mission...).

Pendant

Maîtriser le déroulement de l'entretien n'est pas chose facile. Il faut tout à la fois : poser des questions en gardant le fil conducteur du guide préalablement établi, noter les réponses et remarques des audités, récupérer les documents complémentaires tout en conservant l'attention de l'interviewé afin qu'il ne s'égaré pas dans de futilles considérations, des discours dithyrambiques ou encore ne s'épanche pas trop sur ses « états d'âme » (éviter le cahier de doléances). Cet exercice est par ailleurs à réaliser avec un souci de l'exhaustivité et du détail des informations recueillies et dans un temps imparti. Si l'on n'a pas couvert l'ensemble des points prévus à l'ordre du jour, on ne pourra pas nécessairement programmer un second rendez-vous.

Après

Exercice fastidieux et obscur mais absolument nécessaire, le compte rendu d'entretien. Même si, à titre personnel, l'auditeur « qui pense avoir tout dans sa tête » n'en voit pas toujours l'intérêt, il est indispensable. Une

mission d'audit est un travail d'équipe. À moins que l'équipe complète participe à toutes les interviews (irréaliste compte tenu de la contrainte de temps), les comptes rendus écrits servent à partager l'information entre ses membres. Même très professionnel et expérimenté, l'enchaînement de plusieurs entretiens ne permet pas de se rappeler de tout. La formalisation est une garantie de ne rien oublier.

Figure 8.1 – Schéma d'une interview

 Figure 8.1. Voir l'explication dans le texte.

Avantages/inconvénients (limites) de l'outil

La rencontre directe avec les audités permet à l'auditeur de se forger une première opinion sur le niveau de risque. De plus, l'audité est ainsi impliqué dans la démarche d'audit et il adhérera d'autant plus facilement aux recommandations ultérieures qu'il aura le sentiment d'en avoir été un acteur. Cependant, le bon déroulement de l'interview et donc l'intérêt de cette technique sont basés sur le climat de confiance ou de méfiance qui s'installe entre l'auditeur et l'audité. L'interviewer peut éventuellement être trompé par l'interviewé ou ne recueillir qu'une partie des informations – qui peuvent par ailleurs ne pas être considérées comme des preuves tangibles et seront donc réfutables par les audités.

Les questionnaires administrés

À quoi ça sert ?

Un questionnaire administré est une liste de questions auxquelles on doit répondre par écrit. Les réponses sont généralement reportées par l'auditeur – on parle alors d'« administration indirecte » –, mais il arrive que l'interrogé remplisse lui-même le questionnaire – on parle dans ce cas d'« administration directe ».

On peut classer les questionnaires administrés en deux grandes catégories : d'une part les questionnaires à choix multiples (QCM), où le choix des réponses est limité, d'autre part les questionnaires ouverts (QO), où le

choix des réponses est illimité. Un questionnaire de contrôle interne (QCI) sert principalement lors de la phase d'étude (prise de connaissance du sujet audité). Il constitue une aide très appréciable dans le cadre des entretiens de recueil d'informations auprès des responsables audités en garantissant une exhaustivité des thématiques à aborder.

Quand l'utilise-t-on ?

Le questionnaire s'emploie de deux manières : comme un outil d'analyse uniquement ou comme un outil d'interview et d'analyse. Dans le premier cas, il est rempli par l'auditeur après l'interview à partir des notes qu'il a prises. Dans le second cas, les réponses sont fournies directement par l'interrogé. Il peut être utilisé lors de la phase d'étude comme lors de la phase de vérification pour apprécier la mise en œuvre d'une tâche définie au programme de vérifications.

Comment l'utilise-t-on et qui l'utilise ?

L'organisation du questionnaire relève d'une technique et dépend de la chose que l'on cherche à connaître, c'est-à-dire du domaine audité. Quel que soit le type de questionnaire, l'ordre des questions est un point crucial qui doit être réfléchi. Elles doivent être regroupées par thèmes, suivre un ordre logique (du plus général au plus spécifique) et progresser de façon à mettre en confiance l'audité. Les questions les plus spécifiques et techniques doivent ainsi être abordées au milieu du questionnaire de façon à ne pas effrayer l'audité au début et à ne pas pâtir de sa chute d'attention en fin d'entretien.

On doit poursuivre une démarche redondante dans les questions de façon à croiser les réponses et à s'assurer de la cohérence et de l'exhaustivité des éléments apportés par l'audité. Il peut être utile d'utiliser des questions « à tiroir » afin de s'assurer de l'épuisement du domaine traité. Le questionnaire ne doit pas être trop long car la précision des réponses fournies par les audités diminue en fonction de la durée. La présentation doit être maniable, facile à lire et facile à remplir pour éviter le rejet du questionnaire par l'audité. Les QCM sont plus simples pour les interrogés et plus aisés à dépouiller pour les auditeurs. Ils conviennent

particulièrement pour les audits de conformité, de régularité. À l'inverse, les QO sont plus pertinents pour les audits d'efficacité, de management, ainsi que sur les sujets nouveaux. Sur ce point précis, ils s'apparentent aux questionnaires de contrôle interne.

Avantages/inconvénients (limites) de l'outil

La formulation des questions est un point essentiel et risqué qui jouera sur l'interprétation des réponses (formulation subjective et suggestive) : certaines formulations induisent des réponses particulières et des mots peuvent être chargés affectivement (« erreur », « faute »...). Les questions doivent être rédigées dans le langage de l'audité et pas dans celui de l'auditeur. Il convient donc de tester le questionnaire avant de l'utiliser. Et une formulation correcte à l'écrit peut se révéler inadaptée à l'oral. Il ne faut pas se tromper d'interlocuteur, c'est-à-dire poser une question à un audité qui n'a pas l'information nécessaire pour y répondre. Les QCM permettent une comparaison aisée mais ce n'est pas le cas des QO ni des QCI. L'auditeur cherche toujours à capitaliser l'expérience acquise mais l'emploi de questionnaires types (non actualisés) peut conduire à une situation où les questions ne sont plus adaptées à la réalité de l'objet audité.

EXEMPLE DE QUESTIONNAIRE DE CI POUR LE PROCESSUS « ACHATS »

1 – Commande

Qu'est-ce qui assure que toutes les commandes :

- ne peuvent pas être passées sans l'autorisation de personnes ayant autorité pour cela ?
- offrent des garanties suffisantes quant :
 - au choix des fournisseurs ?
 - aux prix ?
 - aux conditions de règlement ?

- sont suivies ?

2 – Réception

Qu'est-ce qui assure :

- que toutes les réceptions correspondent à des marchandises commandées ?
- que toutes les réceptions sont conformes aux commandes quant :
 - aux quantités ?
 - à la qualité ?
 - à la date de livraison ?
- que toutes les réceptions sont enregistrées et connues des autres services intéressés ?
- que toutes les anomalies sont traitées ?

3 – Enregistrement comptable

Qu'est-ce qui assure :

- qu'il est gardé une trace de la réception des factures ?
- que toutes les factures reçues se rapportent à des marchandises ou services effectivement reçues ?
- que toutes les factures sont conformes à la commande quant :
 - aux prix ?
 - aux conditions de règlement ?
- que toutes les factures sont comptabilisées ?

- que toutes les factures sont contrôlées arithmétiquement ?
- que la comptabilisation des factures est rapide ?
- qu’une double comptabilisation des factures est impossible ?
- que le service comptable a connaissance des marchandises ou services reçus dont les factures ne sont pas encore parvenues ?
- que toutes les anomalies concernant le contrôle des factures sont traitées ?

4 – Paiement des factures

Qu’est-ce qui assure :

- que tout paiement est justifié par une facture acceptée ?
- que le « bon à payer » est donné par des personnes ayant autorité pour cela ?
- qu’un double paiement des factures est impossible ?
- que les acomptes et les avoirs sont déduits des paiements ?

5 – Avoirs

Qu’est-ce qui assure :

- que tous les retours de marchandises sont enregistrés et qu’ils sont connus des autres services intéressés ?
- que tout retour ou litige donne lieu à l’émission d’un avoir ?
- qu’il est gardé une trace de la réception des avoirs ?
- que tous les avoirs sont corrects quant :
- aux quantités retournées ou litigieuses ?

- aux prix mentionnés sur les factures initiales ?
- que tous les avoirs sont comptabilisés ?
- que la comptabilisation des avoirs est rapide ?
- qu’une double comptabilisation des avoirs est impossible ?
- que le service comptable a connaissance des retours ou litiges pour lesquels les avoirs ne sont pas encore parvenus ?
- que toutes les anomalies sont traitées ?

6 – Comptes fournisseurs

Qu’est-ce qui assure :

- que tous les comptes fournisseurs sont analysés régulièrement ?
- que toutes les anomalies sont traitées ?
- que la cohérence entre la balance des comptes fournisseurs individuels avec le compte collectif fournisseur est établie ?

La piste d’audit

À quoi ça sert ?

La piste d’audit recouvre deux notions. À l’origine, c’est une technique de contrôle comptable plus particulièrement à l’usage des auditeurs externes (applicable dans le cadre de l’article 103 de la loi 89-935 du 29 décembre 1989 au contrôle fiscal des comptabilités informatisées). C’est par ailleurs une technique d’audit à laquelle les auditeurs internes ont largement recours. Ce texte de loi et différentes réglementations professionnelles définissent la piste d’audit comme « *un ensemble de procédures permettant de justifier toute information en remontant du*

document de synthèse à la source par un cheminement ininterrompu et réciproquement ». Elles doivent couvrir :

- la reconstitution de l'ordre chronologique des opérations ;
- la traçabilité ascendante et descendante (piste d'audit statique) ;
- la justification d'une information d'une date à l'autre (piste d'audit dynamique) ;
- la conservation des données : reconstitution du chemin de révision à partir des données conservées et justification de ces données à partir des règles de gestion.

Quand l'utilise-t-on ?

Lors de la phase de lancement de la mission sur site afin d'identifier les faiblesses potentielles du contrôle interne. Lors de la phase de conduite des vérifications afin de récupérer les preuves matérielles attestant des faiblesses avérées du contrôle interne.

Comment l'utilise-t-on et qui l'utilise ?

Lors de la phase de lancement de la mission sur site, et plus précisément dans le cadre de l'élaboration du programme de vérification, l'auditeur interne va pouvoir, en suivant la piste d'audit, reconstituer le cheminement des étapes du processus audité. Grâce aux informations récupérées auprès des audités lors d'interviews (séquence et nature des opérations réalisées, responsables concernés, documents utilisés, dates et lieux des opérations, conservation des informations...), l'auditeur dispose des informations nécessaires à l'identification des faiblesses potentielles du contrôle interne. Lors de la phase de conduite des vérifications, l'auditeur interne, dans le cadre des tests qu'il réalise, s'assure, en suivant la piste d'audit, de l'existence et de la pertinence de tous les éléments caractérisant les opérations réalisées. L'absence, l'insuffisance ou l'inadéquation de ces éléments, au regard des bonnes pratiques de contrôle interne, constitueront

pour l'auditeur interne des preuves tangibles des dysfonctionnements avérés.

Avantages/inconvénients (limites) de l'outil

En tant que dispositif de contrôle interne, la mise en place de la piste d'audit concourt à sécuriser les informations et à assurer la traçabilité des opérations réalisées afin d'en faciliter le suivi et le contrôle. En tant que technique d'audit, remonter la piste d'audit permet à l'auditeur d'avoir une approche détaillée et exhaustive du domaine audité. Cette méthode d'investigation est cependant très consommatrice de temps dans le cadre d'une mission d'audit. Elle est probablement à utiliser lorsque les circonstances l'exigent, c'est-à-dire lorsque le risque supposé est jugé important. Par ailleurs, ce mode de réflexion ne doit pas conduire l'auditeur à ne porter son jugement qu'à travers les pratiques en vigueur en oubliant d'autres pratiques de contrôle interne plus pertinentes.

Exemples de piste d'audit

Opérations relatives à la vente d'un produit

 Illustration. Voir l'explication dans le texte.

 Illustration

Opérations relatives à l'achat d'un bien

 Illustration. Voir l'explication dans le texte.

Les observations physiques

À quoi ça sert ?

L'observation physique est la constatation de la réalité instantanée de l'existence et du fonctionnement d'un phénomène (en audit, on observera un processus, une transaction, un site, un bien, des documents, des

comportements...). L'auditeur qui observe attentivement soulève souvent des problèmes qui ne sont pas connus, ou qui ne peuvent être déduits de l'analyse de l'information écrite. L'observation est aussi une source riche d'exemples spécifiques qui sont utiles à l'illustration des conclusions générales.

Quand l'utilise-t-on ?

L'observation physique est pratiquée par les auditeurs internes lors de la phase de lancement de la mission afin de bien appréhender le contexte audité, et en phase de vérification afin éventuellement d'obtenir des preuves probantes de faiblesses avérées.

Par exemple, en phase de lancement, il peut être intéressant, à la fin d'un entretien dans lequel une procédure a été décrite, d'essayer de résumer sa compréhension en demandant à l'interlocuteur de prendre un exemple et d'en suivre le cheminement. De la même manière, une visite de l'entité auditée est très souvent significative de l'environnement dans lequel se déroulent les activités. Des éléments tels que la propreté et le rangement des aires de production, la signalétique des bureaux, le signalement, la protection des zones sensibles (sécurité des personnes, confidentialité des informations) sont autant de signes précurseurs de la qualité du management de l'entité.

Comment l'utilise-t-on et qui l'utilise ?

L'observation physique doit être pratiquée par l'ensemble des auditeurs, de l'auditeur junior jusqu'au chef de mission. Afin de bien pratiquer les observations physiques et surtout de pouvoir se servir des résultats dans la suite de la mission, il est important de les noter et sauvegarder dans l'instant. Si rien n'est marqué après une observation intéressante, on retombe dans les aléas de la mémoire et on enlève de la force probante à l'observation. Plus l'enregistrement formel d'une observation tardera, plus on affaiblira la solidité du constat.

La seconde bonne pratique de l'observation physique consiste à observer à plusieurs personnes. Cela a pour but d'éliminer la subjectivité de

l'observation qui subsiste toujours. C'est pourquoi en théorie les auditeurs devraient marcher, et surtout, observer par deux. L'observation peut aussi être indirecte. Il s'agit de vérifier l'existence d'un élément (un bien, une relation contractuelle avec un tiers...), soit par la consultation directe des documents (authentiques au sens juridique) qui en attestent, soit par correspondance avec les tiers concernés (circularisation des clients, lettre de confirmation de banque, certificat de conservation des hypothèques...).

Avantages/inconvénients (limites) de l'outil

L'observation physique est bien évidemment la technique qui présente les garanties les plus solides : il n'est rien de plus fiable que le phénomène observé directement par l'auditeur interne. Cependant cette technique d'audit n'est pas universelle :

- elle n'est pas toujours possible (nécessité de disposer de connaissances techniques spécifiques hors du champ de compétences de l'auditeur, lieu de l'observation inapproprié, période de l'observation incompatible avec le planning de la mission...) ;
- une observation physique faite sur un élément donné et à un instant donné ne permet pas de généraliser le constat à toute une population.

Les rapprochements et reconstitutions

À quoi ça sert ?

Le *rapprochement* est la vérification ponctuelle et *a posteriori*, par d'autres sources ou moyens, de la validité d'un fait, d'une affirmation ou d'une déclaration. Les sources ou moyens peuvent être à la fois de nature exogène (confirmation écrite extérieure) ou endogène (supports d'informations dans la chaîne d'un processus). Par exemple :

- le rapprochement bancaire ;
- le rapprochement entre l'inventaire physique et l'inventaire comptable.

La *reconstitution* est le rétablissement d'un résultat à partir d'éléments réels et pertinents, soit par utilisation du processus lui-même, soit par mise en œuvre de processus différents mais homologues au phénomène contrôlé.

Par exemple :

– le processus de recrutement : 1) Besoin, 2) Recherche/sélection du candidat, 3) Contrat, 4) Intégration, 5) Versement du salaire ;

– le processus d'achat : 1) Besoin, 2) Identification/sélection du fournisseur, 3) Contrat, 4) Réception, 5) Vérification, 6) Règlement.

Quand l'utilise-t-on ?

Le rapprochement est utilisé en audit de conformité, afin de vérifier un fait ou une affirmation d'une ou plusieurs opérations. La reconstitution est utilisée en audit d'efficacité, afin d'évaluer le fonctionnement et/ou la fiabilité d'un système, d'un processus.

NB : la reconstitution peut être utilisée pour valider un fait alors que le rapprochement ne permet pas l'évaluation de la fiabilité ou du fonctionnement d'un système.

Comment l'utilise-t-on et qui l'utilise ?

Le rapprochement peut se faire à travers deux mécanismes :

- la concordance : soit totale et instantanée – vue d'ensemble immédiate (par exemple, le magasinier rapproche bons de livraison et bons de réception) –, soit progressive – donnée après donnée (par exemple, le comptable effectue les rapprochements bancaires) ;
- la confrontation : soit conçue par l'auditeur, soit réalisée par l'audité, soit fournie par un tiers.

Le rapprochement peut être une simple observation physique.

La reconstitution consiste à refaire un processus de flux d'informations (théoriques ou réels), afin d'obtenir un résultat attendu, dans le but de s'assurer du bon fonctionnement et le cas échéant, de mesurer les écarts. Ainsi, la reconstitution valide soit les flux, soit le processus, soit les faits. La reconstitution est réalisée uniquement par l'auditeur, sur la base d'éléments fournis par l'audité.

Avantages/inconvénients (limites) de l'outil

Le rapprochement :

- ne nécessite aucune connaissance approfondie de l'organisation ;
- facilite le suivi des processus ;
- est facile à mettre en place.

Néanmoins, il ne permet pas l'évaluation du fonctionnement et de la fiabilité d'un processus, d'un système.

La reconstitution :

- offre une vision globale et détaillée du processus ;
- favorise la détection de toute défaillance ;
- peut valider un fait, une situation.

Toutefois, la principale limite de la reconstitution est qu'elle nécessite une connaissance approfondie de l'organisation.

L'interrogation des fichiers informatiques

À quoi ça sert ?

L'interrogation des fichiers informatiques sert à collecter des informations afin de constituer des preuves d'audit. Ces preuves d'audit peuvent

concerner :

- l'existence et l'exactitude des données ;
- l'exhaustivité de ces données ;
- leur accessibilité aux personnes concernées ;
- le respect des délais de production ;
- leur mise à jour et leur suivi.

Quand l'utilise-t-on ?

Cette technique d'audit est à retenir en priorité dès lors que les informations que l'auditeur souhaite contrôler sont mémorisées dans les bases informatiques de l'entité auditée.

Comment l'utilise-t-on et qui l'utilise ?

Concernant ces techniques d'audit assistées par ordinateur, on peut distinguer trois principales modalités d'utilisation :

- l'équipe d'audit peut solliciter les experts des systèmes d'informations (SI) de l'entité auditée afin qu'ils réalisent les requêtes informatiques nécessaires aux contrôles réalisés. Cela nécessite évidemment la disponibilité des experts SI et une bonne collaboration entre auditeurs et audités ;
- l'auditeur peut réaliser lui-même ces requêtes directement à partir des logiciels existants dans l'entité. Cela demande une expertise des auditeurs dans le domaine et une bonne entente avec les audités ;
- enfin l'équipe d'audit peut utiliser ses propres logiciels d'interrogation de bases informatiques (de nombreux produits du marché sont disponibles) dans la mesure où le service d'audit en est doté. Ces logiciels récupèrent les données dans les bases informatiques de l'entité auditée et effectuent tous

les traitements nécessaires dans le cadre d'une mission. Ils sont d'une efficacité redoutable et ne nécessitent pas un investissement en temps très important pour s'y familiariser. À un degré moindre, mais pas sans intérêt malgré tout, les logiciels Excel (fonctions avancées) et de bases de données restent également des outils de traitement des données très intéressants en audit.

Avantages/inconvénients (limites) de l'outil

Avantages :

- augmentation des possibilités d'analyse ;
- amélioration de la qualité des travaux réalisés ;
- application homogène des techniques et des procédures d'audit ;
- optimisation du ratio résultats/coûts, les techniques automatisées étant réutilisables et extensibles ;
- exhaustivité des contrôles ;
- gain de temps considérable lors des contrôles ;
- transportabilité des données.

Inconvénients :

- il faut s'assurer de la fiabilité du système d'information afin d'avoir des données exploitables ;
- toutes les données à contrôler ne sont pas nécessairement mémorisées dans des bases de données informatisées ;
- peut nécessiter des compétences informatiques spécifiques à l'auditeur.

Pour accompagner cette démarche, de nouveaux outils se développent autour des notions de *data analytics*. Pour approfondir ce sujet, le lecteur se

reportera utilement au chapitre 9.

Les sondages statistiques

À quoi ça sert ?

Les sondages statistiques permettent d'obtenir les preuves d'un dysfonctionnement concernant une population nombreuse de plusieurs milliers d'individus (la population « mère ») en observant les faits sur un sous-ensemble réduit de cette population (l'échantillon). Dans le cadre d'une mission d'audit (contrainte de temps), ils rendent ces contrôles réalisables alors qu'un contrôle exhaustif serait inenvisageable car trop consommateur de temps. Cependant, en ne contrôlant qu'un échantillon (quelques pourcents de la population « mère »), les résultats d'un sondage statistique sont entachés de deux incertitudes :

- un niveau de confiance (90 %, 95 %, 99 %), c'est-à-dire le degré de certitude avec lequel l'auditeur annonce le résultat ;
- un intervalle de confiance, c'est-à-dire la fourchette plus ou moins large dans laquelle se situe le résultat réel qui ne pourrait être connu qu'à travers un contrôle exhaustif.

Quatre étapes jalonnent le déroulement d'un sondage statistique.

1. Préparation : définition de la population (taille N), de ses éléments constitutifs ou individus, du caractère à estimer et du niveau de confiance souhaité (noté P). Le choix du niveau de confiance est lié à l'importance du phénomène étudié (95 % niveau de confiance standard, 99 % si on souhaite exprimer une quasi-certitude).

2. Échantillonnage : il s'agit de prélever n individus (taille de l'échantillon) parmi N . La détermination de la taille n de l'échantillon est soit liée au temps que l'auditeur peut consacrer à son sondage, soit calculée par des formules mathématiques. Pour le tirage (prélèvement des n individus), on procède soit par tirage aléatoire (n numéros à désigner sur une plage de 1 à N), soit par tirage systématique : on sélectionne les n

individus suivant un pas ($\text{pas} = N/n$) en balayant toute la population. Cependant, ce dernier principe de tirage n'est possible que si la population est rangée suivant un mode de classement indépendant du caractère étudié.

3. Observation : on réalise le contrôle des n individus. Par rapport aux valeurs observées réelles : x_1, x_2, \dots, x_n , on en calcule la moyenne et la dispersion.

4. Extrapolation : les deux paramètres calculés précédemment (moyenne et dispersion sur l'échantillon) nous permettent, par extrapolation mathématique, de formuler un résultat sur la population « mère » suivant la phrase consacrée : « Il y a P chances sur 100 (niveau de confiance) que la vraie valeur du caractère étudié sur la population totale soit comprise entre (valeur mini) et (valeur maxi) (intervalle de confiance). »

Quand l'utilise-t-on ?

Cette technique est plus particulièrement intéressante lors de la phase de vérification. Elle permet à l'auditeur d'obtenir des preuves probantes qui crédibilisent ses constats de dysfonctionnements.

Comment l'utilise-t-on et qui l'utilise ?

L'auditeur utilise cette technique pour apprécier :

- soit une problématique à caractère discontinu : en général deux réponses (Oui/Non) ; par exemple, la facture est valide ou pas, le dossier est complet ou pas, la procédure est respectée ou pas... Il s'agit des *sondages d'estimation de proportions* ;
- soit une problématique à caractère continu : le phénomène étudié peut prendre une infinité de valeurs ; par exemple, une valeur totale de stocks à une date donnée, un montant de facturation sur une période définie, un montant global du poste « clients » à une date donnée... Il s'agit des *sondages d'estimation de valeurs*.

Avantages/inconvénients (limites) de l'outil

Cette technique réduit considérablement le temps, donc le coût des investigations, tout en apportant une valeur mathématiquement probante aux preuves obtenues. Le niveau et l'intervalle de confiance, ainsi que la taille de l'échantillon (directement liée au temps nécessaire au sondage) sont mathématiquement liés. Ce lien permet d'adapter le temps que l'auditeur souhaite consacrer au sondage à l'importance du problème étudié (enjeux financiers). Cet outil est à proscrire si les éléments que souhaite contrôler l'auditeur sont mémorisés dans des bases de données informatisées (système informatique de l'entité auditée). Dans ce cas, des logiciels spécifiques d'interrogation des bases de données (type ACL ou Idéa) doivent être utilisés car ils permettent un contrôle exhaustif dans des temps minimums. Pour accompagner cette démarche, de nouveaux outils se développent autour des notions de *data mining* et d'intelligence artificielle. Pour approfondir ce sujet, le lecteur se reportera utilement au chapitre 9.

L'Essentiel

- Certains outils constituent des compléments indispensables à la méthodologie et l'auditeur interne, en tant que professionnel, se doit de les connaître et de les utiliser à bon escient afin d'améliorer la qualité de ses prestations.
- Au-delà des outils « traditionnels » (analyses, enquêtes, interviews, pistes d'audit, *flow charts*...) émergent ceux issus des nouvelles technologies, développés au chapitre suivant.



Chapitre 9

Les nouveaux outils liés aux évolutions technologiques

EXECUTIVE SUMMARY

- Dans ce chapitre, nous allons aborder les nouveaux outils mis à la disposition des auditeurs et des entreprises grâce aux évolutions liées au numérique, dont nous entendons de plus en plus parler mais que les entreprises utilisent peu.
- Nous allons présenter de manière simplifiée leurs fonctionnements, les risques liés et les enjeux pour les auditeurs.
- L'approche outillée de l'audit sécurise et documente la démarche, renforce sa traçabilité et garantit la pérennité des faits relevés.
- Sans oublier la nécessité de maîtriser l'accès à l'information dans un contexte où se multiplient les applications SaaS, en particulier.

UNE APPROCHE CONTEMPORAINE DE L'AUDIT

Les risques contemporains requièrent l'usage d'applicatifs de plus en plus sophistiqués. Dans la première partie de l'ouvrage, nous avons

indiqué comment l'environnement de l'audit a évolué tant en termes d'objectifs qu'en termes de périmètre audité, nous conduisant de l'audit des comptes vers un audit plus large des organisations et des risques (voir [chapitre 2, figure 2.1](#)).

Vue sous l'angle applicatif, cette évolution milite pour la mise à disposition d'outils qui permettront d'accéder rapidement :

- aux informations propres à l'organisation (organigrammes, gestion des droits) ;
- aux indicateurs de performance et *data* portés par le SI ;
- aux risques identifiés restituables au travers de cartographies multiaxes.

Nous avons proposé dans la deuxième partie un cadre méthodologique sous forme d'un processus de conduite de mission auquel nous avons adjoint les supports et documents associés.

En termes IT, cela induit l'utilisation d'applicatifs permettant :

- de piloter et suivre la mission (*workflow*, Gantt, PERT, tableaux de bord) ;
- d'accéder en temps réel aux supports documentaires, méthodologiques et de *reporting*.

Enfin, dans cette troisième partie dédiée aux outils de l'audit, nous avons insisté ([chapitre 8](#)) sur la nécessité d'appréhender correctement les données économiques et volumétriques (poids relatif et enjeux) en s'attachant aux processus d'élaboration de ces informations (diagramme de circulation des documents, piste d'audit, grille de séparation des tâches, fichiers informatiques...).

Il nous faut ainsi des applicatifs qui permettent :

- de visualiser les processus métiers existant en s'assurant qu'ils sont bien appliqués (outils de *business process management* et de *workflow*) ;
- de visualiser les droits informatiques (cartographies applicatives).

Ces besoins exprimés peuvent être traités en silo et pour partie par des solutions de type :

- BPA (*business process architecture* ou *analysis*) qui sont des outils de modélisation des processus de l'entreprise ;

- IBPMS (*intelligent business process management suites*) et *workflow* qui vont permettre d'exécuter lesdits processus ;
- GRC (gestion du risque et de la conformité), qui vont servir à cartographier les risques liés à l'organisation ;
- BAM (*business activity monitoring*), et BI (*business intelligence and analytics platforms*) qui vont permettre en particulier de générer des *reportings* et indicateurs de performances ;
- GED (gestion électronique de documents) ou ECM (*entreprise content management*) qui vont donner accès à la documentation utilisée par l'organisation.

Ces solutions sont aujourd'hui matures, mais leur orchestration en un seul applicatif visant à couvrir les besoins du SIGR (système d'information de gestion du risque) reste marginale.

Par ailleurs, les *risk managers*, selon la dernière étude de l'AMRAE, demeurent insatisfaits quant à l'interopérabilité de ces solutions avec leurs environnements applicatifs ; l'absence d'API (y compris web services) à l'heure pourtant où se développe toute une gamme de solutions de RPA (*robotic process automation*) semble anachronique.

Figure 9.1 – Résultats de l'étude AMRAE

 Figure 9.1. Voir l'explication dans le texte.

Source : AMRAE, panorama, 11^e édition, 2019.

C'est moins le sujet technique de l'API (*applications programming interface*) permettant de connecter des applications entre elles qui pose problème, que celui de l'identification des droits et autorisations – qui peut, et à quel titre, accéder à telle ou telle information ou transaction.

Ce sujet est rendu complexe par le fait que l'architecture des droits d'un applicatif à l'autre ne répond pas à la même logique.

À titre d'exemple, les droits d'accès aux applications de type CRM (*customer relationship management*) suivent une logique géographique/territoriale, gamme de produit, type de client et fonction hiérarchique de l'utilisateur, quand dans le même temps son accès au suivi des paramètres de paie se contente de relever sa dépendance

hiérarchique et sa fonction ; interfacer les droits nécessiterait un référentiel unique à défaut de nécessiter un traitement lourd de « mise en équivalence » et de suivi.

Ce sujet d'authentification et plus largement de gestion des droits et autorisations est central dès lors que les systèmes d'information sont délégués aux métiers au détriment du SI. Il n'est pas simple à traiter car il suppose une modélisation amont et globale des organisations qualifiées. Il se heurte également au sujet sensible de la protection des données qui contraint les entreprises européennes (RGPD).

Deux approches semblent possibles :

- identification en amont des caractéristiques des acteurs, données et flux par une indexation structurée complète et signifiante ;
- analyse *a posteriori* des flux et des données (*big data*).

La seconde approche est aujourd'hui au cœur de la transformation digitale et l'on voit émerger depuis quelques années une multitude d'outil de *data mining* et *data analytics*, intelligence artificielle, *machine learning*.

Le sujet est en devenir et nous vous présentons dans le paragraphe suivant les principales innovations et tendances en la matière.

Véritable tsunami technologique mais également économique et sociétal, ces solutions mettant en œuvre des algorithmes classiques en mathématiques appliquées nécessitent une quantité de données importante (*big data*) ; elles sont intrusives, à la main de l'éditeur, le plus souvent SaaS, et posent le problème prégnant de la protection des données.

C'est donc sans surprise que l'on trouvera ces solutions le plus souvent auprès des GAFA américains et BATX chinois qui y consacrent des investissements colossaux, mais surtout bénéficient d'un accès quasiment illimité et pas ou peu contraints à la donnée.

UNE APPROCHE DES RISQUES INTÉGRANT LA GESTION DES AUTORISATIONS (DROITS, DONNÉES ET SOD)

Risk – Organization – Knowledge

La multiplication des applications digitales a été favorisée par l'émergence en dix ans des solutions *cloud* (SaaS) *multi-device* (mobiles, tablettes...). Leur facilité d'implémentation (pas de schéma directeur informatique, pas d'installation lourde) a délocalisé la décision de leur mise en œuvre et de leur déploiement vers les responsables métiers au détriment souvent du DSI.

Ces applications prennent en charge de plus en plus de traitements de données. Elles peuvent être alimentées par des collaborateurs, mais de plus en plus se substituent aux tâches de *back-office* avec toute une panoplie de robots interconnectés entre eux et/ou avec les autres applications de l'écosystème IT de l'entreprise.

La maîtrise des droits et autorisations est un risque majeur à la main de l'auditeur quand les risques techniques (piratage, intégrité de la donnée, etc.) incombent davantage au DSI.

La proposition apportée par la solution ROK déployée dans des groupes internationaux multi-sites est sur ce point originale et intègre une approche à la fois organique et systémique des organisations.

Intégrant les fonctionnalités classiques de BPA, IBPMS, RPA GED, GRC, BI, etc., en un hub collaboratif unique, l'éditeur intègre une solution de modélisation de l'organisation.

On va ainsi pouvoir piloter très aisément et de façon dynamique la gestion des autorisations applicatives en faisant évoluer manuellement ou dynamiquement (intégration avec l'annuaire électronique) d'un côté l'organisation (entrée, sortie, mobilité des collaborateurs ou acteurs de

l'écosystème) et de l'autre les activités représentées sous forme de *flow charts* connectés au SI.

Dès lors que cette architecture est à la main du métier, il devient aisé à ce dernier de s'assurer que l'accès à l'information et son traitement sont intègres avec l'organisation mise en place.

Figure 9.2 – ROK – Monitoring des autorisations de façon intégrée en fonction des mouvements dans l'organisation et/ou des processus de l'entreprise

 Figure 9.2. Voir l'explication dans le texte.

Le fait de rassembler en une seule vue les acteurs, les activités et les transactions informatiques va permettre d'automatiser et sécuriser à la fois la piste d'audit, mais également de monitorer la séparation des tâches.

Les grilles réalisées plus haut vont pouvoir être interfacées soit avec la tâche normée, soit avec la transaction informatique autorisée ; dès lors, la solution fera apparaître à chaque modification de l'organisation les transactions et activités présentant un risque au regard de l'intégrité de la séparation des tâches.

La représentation des droits et autorisations peut se faire en amont ou en recueil des droits existants. Son monitoring peut se faire dans chaque applicatif (ROK se contentant de représenter le résultat) ou directement dans ROK.

Cet exemple s'inscrit dans la continuité des solutions de SIGR du marché.

D'autres approches totalement disruptives émergent, qui s'appuient sur l'analyse des données ou la mise en œuvre des principes des mathématiques appliquées au travers de solutions d'intelligence artificielle et de *machine learning*.

Les paragraphes suivants dressent un panorama de ces offres en devenir.

LES PRATIQUES ACTUELLES ET ÉVOLUTIONS LIÉES AU NUMÉRIQUE

Afin d'analyser les pratiques actuelles et les évolutions de la méthodologie de l'audit liées au numérique, nous avons sollicité nos étudiants du master « Stratégie, Gouvernance et Audit interne » de l'IAE d'Aix-en-Provence dans le cadre de leurs travaux d'analyse et de recherche. Nous les remercions pour leur contribution. Ils se sont basés sur plusieurs documents récents et dossiers de presse de l'IFACI qui font ressortir des évolutions du métier d'auditeur interne.

L'étude met en exergue l'importance pour l'audit interne de « s'adapter aux nouvelles applications des évolutions technologiques ». En effet, si la banalisation des nouvelles technologies de l'information et de la communication (NTIC) au sein des entreprises est allée de pair avec l'émergence de nouveaux risques, comme par exemple les cyber-attaques, celle-ci a également permis le développement de nouveaux outils tels que le *data analytics*, le *data mining* et l'intelligence artificielle.

Tout comme les audits internes ont construit des pôles de compétences informatiques lorsque l'informatique s'est généralisée dans les entreprises, il semble essentiel de construire des pôles de compétences liées aux usages des données et à leur traitement. Dans un premier temps, pour s'assurer que l'audit reste en mesure de comprendre le fonctionnement de l'entreprise dans laquelle il agit. Dans un second temps, afin d'appliquer aussi à l'audit ses outils. En effet, avoir à disposition des outils permettant de traiter de vastes volumes de données pour en tirer des conclusions et structurer l'information a un intérêt pratique pour l'audit.

Dès lors, comment les auditeurs analysant un processus peuvent-ils s'assurer de la pertinence de la prise de décision par le système ? Il leur sera nécessaire de pouvoir analyser le fonctionnement de l'algorithme de décision (non seulement au niveau de sa conception

« théorique », mais encore au niveau de son implémentation dans le système d'information), ceci requérant des compétences spécifiques.

Par ailleurs, si les services d'audit se doivent de disposer de personnel formé et/ou diplômé, il est aujourd'hui nécessaire d'encadrer la conduite d'une mission d'audit interne *via* un applicatif informatique collaboratif.

L'ANALYSE DES DONNÉES (*DATA ANALYTICS*)

D'un point de vue très générique, le *data analytics* (analyse de données) est une science consistant à examiner des données, dans le but de tirer des conclusions à partir de ces informations.

L'analyse de données est utilisée dans de nombreuses industries et métiers depuis quelques années afin de permettre aux entreprises et organisations de mieux comprendre les flux passés, de prendre de meilleures décisions et de plus en plus pour prévoir des événements futurs *via* l'analyse de données prédictive.

Deux dimensions sont généralement prises en considération concernant l'analyse de données :

- la donnée elle-même (sa nature, son volume, sa présence en entreprise et dans nos vies). La notion de donnée est considérée ici dans un sens large. Elle ne se restreint pas par exemple aux données d'identification ou de caractérisation des employés ou clients, mais est complétée par des sources externes (réseaux sociaux, bases de données publiques ou privées) aux formats très variés (vidéos, textes, « tweets », photos) ;
- les traitements que l'on en fait (par exemple les algorithmes qui sont utilisés, leur complexité, leur interprétabilité).

Les sujets d'analyse de données se sont considérablement imposés dans les débats de la vie économique et de la vie publique.

Deux tendances se sont renforcées dans la dernière décennie :

- les données sont devenues omniprésentes et archi-volumineuses (*big data* ou grand volume de données) ;
- les algorithmes sont devenus de plus en plus complexes (par exemple ceux basés sur l'analyse en réseaux de neurones) et sont développés dans une logique « apprenante » autonome, laissant à la machine une prérogative auparavant humaine.

Dans le prolongement de ces tendances, on constate actuellement qu'il y a deux phases disruptives et durablement installées :

- l'exploitation systématique des données, à des fins commerciales ou de contrôle ;
- l'automatisation de certaines tâches humaines.

Des modes de traitement et d'utilisation de ces données se mettent en place dans des dimensions différentes, mais dans une logique de *continuum* autour d'une utilisation plus ou moins poussée de la donnée.

Par exemple, pour simplifier il est possible de :

- décrire les données récoltées, les classer et les analyser. Cette description peut être plus ou moins complexe selon le nombre de données traitées, et la complexité des traitements qui vont opérer pour obtenir la description voulue. Ainsi, la sémantique de *big data* est liée à ces processus de description, mais pour un grand volume de données ou selon la complexité des traitements qui vont être nécessaires ;
- utiliser des algorithmes simples que tout un chacun peut maîtriser (ex. : « arbre de décision » dont on fixe les valeurs sur la base d'un processus maîtrisé, et qu'on cherche à répéter ou à automatiser). C'est actuellement dans ce contexte que l'on déploie les robots. C'est de la robotique ;
- utiliser des algorithmes simples, mais moins contrôlables (ex. : *Random Forest*, qui sont des arbres de décision, mais moyennés, et avec une dose de hasard dans l'apprentissage). C'est du *machine learning* ;
- enfin, dans le prolongement de la complexité, l'intelligence artificielle utilise tous les axes, et notamment la notion d'apprentissage.

Quels impacts a le *data analytics* sur les métiers de l'audit et du contrôle interne ?

Le *data analytics* correspond à l'analyse de données brutes dans le but d'émettre des conclusions qui sont notamment utilisées dans le cadre de l'analyse des *big data* et qui correspondent à une très grande quantité de données stockées sur une base numérique. Ainsi, les départements d'audit interne sont désormais en train d'intégrer pleinement l'utilisation de ces nouveaux outils au sein de leur méthodologie d'audit.

Ceci se matérialise notamment en recrutant des collaborateurs ayant de solides compétences informatiques ainsi qu'en proposant des formations IT aux collaborateurs, afin qu'ils soient capables, d'une part d'auditer l'utilisation de ces nouveaux outils par les opérationnels et donc d'aider l'organisation à en faire un usage optimal, et d'autre part d'utiliser ces outils de *data analytics* durant leurs missions d'audit.

Le *data analytics* ne vient pas « prendre la place » des auditeurs mais modifie profondément leur manière de travailler. En effet, si auparavant l'auditeur utilisait beaucoup la technique des sondages statistiques afin d'obtenir, à partir d'un échantillon représentatif d'une population globale, des conclusions extrapolables à cette population globale, les outils de *data analytics* et de *big data* permettent à présent de faire une analyse exhaustive de quantités de données beaucoup plus importantes que ce que pourrait analyser manuellement une équipe d'audit.

Ceci se traduit donc par un gain de temps pour les équipes d'audit mais également par une meilleure qualité des travaux d'audit. En effet, la revue exhaustive de grandes quantités d'informations permet aux missions d'audit, interne de couvrir un plus grand champ d'investigation et donc de venir réduire les zones de risques auxquelles est exposée l'organisation.

Grâce au *data analytics*, l'audit interne devrait être « plus efficace et plus pertinent », car il lui sera désormais possible de réaliser des analyses des risques avec une perspective beaucoup plus macro.

Ainsi, grâce à ces nouvelles technologies, les services proposés par l'audit interne sont donc amenés à évoluer et son rôle sera désormais de plus en plus d'aider l'organisation avec des analyses qui soutiennent l'information de prise de décision.

Trois enjeux peuvent être considérés s'agissant du *data analytics* : l'impact pour les métiers du contrôle, les impacts que cette évolution apporte sur les modèles économiques et sur les processus des entreprises dans lesquels les fonctions de contrôle opèrent.

Pour le premier enjeu – les professionnels de l'audit et du contrôle interne –, l'analyse de grands volumes de données se traduit par des opportunités de modifier les modes de travail en traitant par exemple des tests d'efficacité des contrôles de façon systématique et non plus par échantillon.

Pour le contexte de leur métier, cela implique aussi que ces fonctions de contrôle soient au fait des évolutions que l'analyse de données peut produire pour l'entreprise et le contexte économique dans lequel elle opère.

En quelque sorte, l'analyse de grands volumes de données est le premier maillon de la digitalisation pour l'entreprise et les fonctions d'audit et de contrôle. Les attentes sont différentes et variées entre les besoins de l'opérationnel qui commence à s'investir dans la démarche, pour ses besoins, et les besoins des fonctions de maîtrise des risques qui doivent d'une part acquérir la démarche, mais aussi avoir l'assurance que celle développée par les opérationnels est efficace et répond bien au besoin du dispositif de contrôle interne de l'entreprise.

La qualité des données utilisées et restituées et la revue de la démarche d'analyse développée sont ainsi des éléments des processus à réaliser pour permettre à l'auditeur ou au contrôleur interne d'utiliser les travaux des opérationnels dans l'évaluation des dispositifs de contrôle interne.

Dans une démarche basée sur l'utilisation de grands volumes de données, avec les outils technologiques puissants qui en sont le corollaire, on passe d'une analyse à base d'échantillons à l'intégralité des données et on regarde ce qui s'écarte d'une norme (jour, heure...) selon des règles déjà connues.

Les outils peuvent aussi effectuer des analyses statistiques pour constituer une référence, identifier des transactions qui s'écartent des cas normaux, possibles erreurs ou schémas frauduleux. On passe alors de règles prescrites à de la recherche automatique, dans l'objectif d'une meilleure identification des zones de risques de l'entreprise.

L'analyse de grands volumes de données va se limiter à des démarches machines qui vont rester simples sans couche logicielle supplémentaire telles *business intelligence*, intelligence artificielle, *blockchain* ou *robotics*. La première problématique concrète sur lesquels des progrès ont été faits pour aider les processus des fonctions de contrôle est souvent le risque de fraude.

Globalement, c'est une première étape technologique dans la transformation des fonctions audit et contrôle. Ainsi par exemple, par rapport aux règles métiers, le seuil peut être mis par la machine. Le système peut également proposer des règles qui se rapprochent des règles frauduleuses identifiées et on cherche alors des analogies sur les types d'écritures par exemple ; ou encore, le système identifie des corrélations entre variables et la machine va trouver des similitudes – mais celles-ci ne sont pas forcément faciles à interpréter.

L'EXPLORATION DES DONNÉES (DATA MINING)

Le *data mining* se nourrit comme le *data analytics* de la donnée portée par le(s) système(s) d'information(s) et/ou le web.

Mais au-delà de remonter l'information brute pour l'exposer au traitement, le *data mining* va intégrer les données transactionnelles, les métadonnées et *patterns* applicatifs, donnant ainsi une vue organisée des flux.

La relation opérationnelle ou fonctionnelle des données entre elles est centrale dans cette approche, de même que l'indexation pertinente de ces données (qualification, sens de la donnée).

Des algorithmes (mathématiques appliquées) vont aider à segmenter la population globale analysée en populations homogènes autorisant la mise en place de *machine learning*, par exemple.

Il n'y a pas de réelle innovation si ce n'est que l'extraction, le stockage (*datawarehouse*) et le calcul sont rendus exhaustifs et rapides et le sondage classique obsolète.

Plus le support initial de la donnée est structuré et indexé, plus l'information devient pertinente et utilisable ; si je sais que le produit P fait partie de la gamme de produits G et que cette gamme est à destination de la cible C, je commence à avoir une donnée structurée qui va pouvoir être exploitée.

L'auditeur trouvera là un outil intéressant lui permettant de visualiser la normalité ou pas de transactions et comportements, ainsi que les risques liés à la circulation de l'information entre les mains de collaborateurs dans l'entreprise (séparation de tâches en particulier).

L'outil pourra avantageusement être « collé » aux outils de BPM, *workflow* ou RPA au sein de l'entreprise.

Si de surcroît l'annuaire électronique est accessible et renseigné, l'information va prendre de la valeur et pouvoir être avantageusement exploitée par l'auditeur.

On est typiquement dans une approche organique et systémique des organisations et des transactions, dont on trouve trace dans les travaux d'audit, logigrammes et autorisations décrites en parties I et II.

Le *data mining* s'entend ainsi comme un outil prolongeant le *data analytics* et ouvrant la voie au *machine learning* et à l'IA.

L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle est un terme général qui désigne les technologies rendant les machines « intelligentes ». Les organisations investissent dans la recherche sur l'intelligence artificielle et ses applications pour automatiser, accroître ou reproduire l'intelligence humaine, c'est-à-dire les compétences analytiques et/ou la prise de décisions humaines.

La profession d'audit interne doit être prête à participer pleinement aux initiatives des organisations en matière d'intelligence artificielle. Il existe de nombreux concepts associés à l'intelligence artificielle comme l'apprentissage profond, l'apprentissage automatique, la reconnaissance d'image, le traitement du langage naturel, l'informatique cognitive, l'amplification de l'intelligence, l'augmentation cognitive, l'intelligence augmentée grâce aux machines. L'intelligence artificielle, dans le sens où nous l'entendons ici, englobe l'ensemble de ces concepts.

L'intelligence artificielle est alimentée par des algorithmes, qui sont eux-mêmes alimentés par le *big data*. Par conséquent, avant qu'une organisation se lance dans l'intelligence artificielle, et avant que l'audit interne ne puisse traiter l'intelligence artificielle, ils devraient tous deux avoir de solides bases concernant le *big data*.

Le *big data* signifie bien plus que de grands volumes de données. Il fait référence à des données (informations) qui atteignent un volume, une variété, une vélocité et une variabilité si importants que les organisations investissent dans des architectures de système, des outils et des pratiques spécifiquement conçus pour les gérer. Une grande partie de ces données peut être générée par l'organisation elle-même, tandis que d'autres données peuvent être publiques ou achetées auprès de sources externes.

Pour faire bon usage du *big data*, les organisations élaborent des algorithmes. Un algorithme est un ensemble de règles que la machine doit suivre. Il permet à une machine de traiter rapidement de grandes quantités de données qu'un être humain ne pourrait raisonnablement pas traiter ou même comprendre.

La performance et l'exactitude des algorithmes sont essentielles. Ces derniers sont initialement élaborés par des hommes, c'est pourquoi leur performance peut être affectée par les erreurs et les biais humains (intentionnels ou non).

Des algorithmes défectueux peuvent produire des bogues indésirables dans les opérations des organisations, voire de véritables catastrophes. Il est largement admis que des algorithmes défectueux sont, du moins en partie, responsables de la crise financière mondiale de 2008.

AUDIT INTERNE ET INTELLIGENCE ARTIFICIELLE (IA)

L'audit interne est apte à évaluer et comprendre les risques et les opportunités concernant la capacité d'une organisation à atteindre ses objectifs. En tirant profit de cette expérience, il peut aider une organisation à évaluer, comprendre et communiquer la mesure dans laquelle l'intelligence artificielle aura un effet (négatif ou positif) sur la capacité de cette organisation à créer de la valeur à court, moyen ou long terme.

L'audit interne peut s'engager dans au moins cinq activités critiques et distinctes liées à l'intelligence artificielle :

- pour toutes les organisations, l'audit interne devrait inclure l'intelligence artificielle dans son évaluation des risques et envisager la possibilité de l'inclure également dans son plan d'audit fondé sur une approche par les risques ;
- pour les organisations qui envisagent l'intelligence artificielle, l'audit interne devrait participer activement aux projets d'intelligence artificielle dès leurs débuts, en fournissant des conseils et des points de vue qui contribuent à la réussite de leur mise en œuvre.
- Cependant, pour éviter toute atteinte perçue ou réelle à son indépendance et à son objectivité, l'audit interne ne devrait pas être chargé, ni être responsable, de la mise en œuvre des processus, politiques ou procédures d'intelligence artificielle ;
- pour les organisations qui ont mis en œuvre certains aspects de l'intelligence artificielle, que ce soit dans leurs opérations (par exemple, un fabricant qui a recours à des robots sur une chaîne de production), ou dans un produit ou service (par exemple, un détaillant qui personnalise les offres de produits en se basant sur l'historique des achats), l'audit interne devrait fournir une assurance sur la gestion des risques liés à la fiabilité des

algorithmes sous-jacents et des données sur lesquelles reposent les algorithmes ;

- l'audit interne doit s'assurer que les questions éthiques et morales qui peuvent entourer l'utilisation de l'intelligence artificielle par l'organisation sont traitées ;
- comme pour l'utilisation de tout autre système majeur, les structures de gouvernance appropriées doivent être mises en place et l'audit interne peut donner une assurance dans ce domaine.

Indépendamment des activités spécifiques effectuées, l'audit interne est bien placé pour jouer un rôle clé dans les activités entreprises par l'organisation dans le domaine de l'intelligence artificielle.

L'audit interne :

- comprend les objectifs stratégiques de l'organisation et les processus mis en œuvre pour atteindre ces objectifs ;
- est en mesure d'évaluer si les activités d'intelligence artificielle réalisent leurs objectifs ;
- peut fournir une assurance interne sur les activités de management des risques de la direction générale pertinentes au regard des risques de l'intelligence artificielle ;
- est perçu comme un conseiller de confiance pouvant soutenir l'adoption de l'intelligence artificielle pour améliorer les processus de l'organisation ou l'offre de produits et de services.

L'audit interne devrait aborder l'intelligence artificielle comme il traite les autres domaines, c'est-à-dire avec une approche systématique et méthodique afin d'évaluer et d'améliorer l'efficacité des processus de management des risques, de contrôle et de gouvernance liés à l'intelligence artificielle.

L'APPORT D'UNE SOLUTION DE TYPE HUB COLLABORATIF POUR PILOTER UN AUDIT INTERNE

Les points abordés ci-avant ont traité de l'impact des technologies de l'informatique sur le traitement des données utiles à la réalisation d'un audit.

Un autre challenge consiste à traiter dans un seul applicatif les problématiques de gestion des risques de façon intégrée avec l'organisation, tout en optimisant la mission d'audit qui pourra s'appuyer sur une connaissance capitalisée.

La solution vers laquelle doivent s'orienter les services d'audit doit permettre de respecter les objectifs suivants :

- garantir dynamiquement la cohérence et l'intégrité entre la cartographie des risques, la doctrine et l'organisation de l'entreprise ;
- permettre la mise en œuvre de *self audit on demand* ;
- mettre en place de façon personnalisée la démarche de l'auditeur tout en lui donnant un accès permanent et en temps réel aux informations dont il a besoin (cartographie des risques, *self assessment*, GED) ;
- garantir l'intégrité entre le travail de l'auditeur et l'organisation de l'entreprise ;
- intégrer les données quantitatives véhiculées par l'ensemble du système d'information propre à l'organisation ;
- prendre en compte les risques liés au développement durable.
-

Figure 9.3 – Le casse-tête de l'IT

 Figure 9.3. Voir l'explication dans le texte.

L'apport d'une solution de type hub digital collaboratif va non seulement optimiser la démarche (gain de temps et sécurisation), mais également permettre l'accès à toute l'information dématérialisée existante dans l'entreprise, agir sur l'organisation, diffuser la bonne pratique résultante et mesurer la performance qui en découle.

L'agrégation automatisée de toutes ces données dans le but de servir le contrôle interne n'est pas une option mais une nécessité. Entreprises et éditeurs ne s'y trompent pas. Il faut être à même de modéliser voire

d'automatiser les organisations que l'on contrôle. Il est nécessaire d'intégrer le référentiel de risques à la démarche de l'auditeur et de s'assurer que l'un comme l'autre sont cohérents avec la (les) norme(s) et en lien direct avec l'entité modélisée.

Mais il faut également capitaliser les savoirs et les compétences, s'assurer que le retour d'expérience soit pris en compte et partagé. La démarche se doit d'être collaborative.

Focus

L'informatique n'invente rien, mais permet la standardisation des supports et de la méthodologie, l'automatisation des tâches, leur suivi, la collecte rapide des informations et la restitution sous forme de *reporting*.

La méthodologie « *Risk Organization Knowledge* » que nous avons exposée dans les précédentes éditions de 2010 et 2014 s'inscrit dans cette logique. Pour en savoir plus, visitez le site ROK solution sur <http://www.audit-interne-referentiels-risques.com> et <https://www.rok-solution.fr>

L'Essentiel

- *Data analytics, data mining*, intelligence artificielle...
- Tant de nouvelles technologies qui vont changer notre quotidien ainsi que la manière dont les entreprises interagissent avec leurs parties prenantes. Ces nouvelles technologies représentent de nouvelles opportunités ainsi que de nouveaux risques : la maîtrise de qui fait quoi et d'une façon plus large des droits informatiques.
- Néanmoins, ces nouvelles techniques sont peu connues et encore mal maîtrisées par les auditeurs.

**Partie
4**

**Les référentiels
de risques –
Illustrations
et cas pratiques**

[Les tableaux des risques Chapitre 10](#)

[Illustrations et cas pratiques Chapitre 11](#)

Chapitre 10

Les tableaux des risques

EXECUTIVE SUMMARY

- Nous avons souhaité présenter des exemples de référentiels de risques qui pourront guider l'auditeur interne lors de l'élaboration des tableaux des risques dans le cadre de sa mission.
- Le paragraphe « L'élaboration d'un tableau des risques » au chapitre 6 détaille la démarche de construction de ce document lors de la phase de préparation de la mission.
- Les référentiels présentés ici sont conformes à ce modèle.

LA STRUCTURATION ET LE MODE D'UTILISATION DES RÉFÉRENTIELS

Structuration des référentiels

Nous avons distingué deux approches dans l'utilisation de ces référentiels : l'*approche globale* et l'*approche détaillée* par processus ou domaines de gestion. Sans être exhaustifs et par rapport aux trois domaines d'intervention de l'audit interne, l'approche globale pourrait s'apparenter au regard que doit porter l'auditeur aux dimensions

« gouvernement d’entreprise » et « management des risques » et l’approche détaillée à celle des « processus de contrôle interne ».

Avis d’expert

**Sophie BARANGER – rapporteur du groupe de travail
AMF sur le dispositif de gestion des risques et du contrôle
interne, rédactrice de la préface de la première édition
de cet ouvrage.**

S’appuyant sur de nombreux retours d’expérience, ce recueil propose des référentiels de risques de plusieurs grandes fonctions des organisations telles que la direction générale ou la finance. Ces référentiels répertorient les bonnes pratiques de contrôle interne communément admises et constituent une source d’inspiration utile aux organisations, petites ou grandes, cotées ou non, publiques ou privées, qui cherchent à améliorer leurs processus de gouvernance, de maîtrise des risques et de contrôle interne.

Approche globale

Ce référentiel permet à l’auditeur d’appréhender la dimension contrôle au niveau général d’une entité (filiale, agence, usine, service...) ; en fait au niveau d’un centre de responsabilité qui :

- a des objectifs à atteindre qui lui sont fixés par ailleurs ;
- dispose d’une organisation (moyens humains, matériels, système d’information...) ;
- doit assurer un reporting auprès de son instance de tutelle.

Ce référentiel n’intègre donc pas les problématiques de contrôle interne spécifiques aux étapes jalonnant un processus opérationnel particulier. Ce second éclairage est abordé dans l’approche détaillée présentée ci-après. Cependant, les problématiques de contrôle abordées dans l’approche globale concernent également les quinze processus et/ou domaines présentés ultérieurement. Afin de ne pas répéter ces thématiques pour chaque processus, nous avons opté pour un regroupement dans un seul référentiel utilisable tel quel, quel que soit le processus audité.

Nous avons choisi un découpage du référentiel (colonne de gauche) calqué sur le modèle de contrôle interne dit « Référentiel AMF ». Ce choix nous a paru s’imposer du fait de son origine et donc de sa

légitimité française. Néanmoins, pour ne pas se priver d'une utilisation de cet outil dans une organisation s'inspirant du COSO en matière de contrôle interne, la correspondance entre ces deux modèles est chaque fois précisée.

Approche détaillée par processus ou domaines de gestion

Nous avons ici une série de quinze référentiels de risques, un pour chaque principal processus ou domaine de gestion traditionnellement rencontré dans toute organisation.

Ces référentiels détaillent, pour chaque étape qui jalonne un processus ou pour chaque sous-domaine d'un domaine de gestion, la dimension « activités de contrôle » commune aux deux modèles COSO et AMF.

Il s'agit des items suivants :

- management – direction générale ;
- gestion des ressources humaines ;
- finance – comptabilité ;
- juridique – fiscal ;
- contrôle de gestion – reporting ;
- systèmes d'information ;
- recherche et développement ;
- marketing ;
- achats ;
- gestion des stocks ;
- production ;
- commercial ;
- service après-vente ;
- logistique ;
- qualité – sécurité – environnement.

L'auditeur interne aura donc le choix d'utiliser tout ou partie de ces quinze référentiels en fonction du cas de figure qu'il aura à traiter.

Nous nous sommes placés dans le cas d'une entreprise manufacturière dans toute sa complexité afin de couvrir le champ le

plus large possible. Nous n'avons pas souhaité intégrer, par souci de simplification et de généralisation, les spécificités sectorielles comme celles du monde bancaire ou des assurances ou tout autre secteur ayant, de par ses activités ou ses spécificités en matière de contrôle interne, des différences trop marquées.

Enfin, ces quinze référentiels constituent un ensemble à part entière et ont été élaborés, notamment au niveau du degré de détail retenu pour le découpage de chaque processus, en tenant compte des contraintes de temps d'une mission. Ils peuvent donc être tous déployés dans le cadre d'une seule et même mission d'audit. En d'autres termes, cette bibliothèque de référentiels a été conçue pour une mission d'audit dit « de filiales », « état des lieux » ou encore « *full audit* », durant laquelle tous les processus de l'entité concernée sont audités. Pour une mission d'audit thématique qui porterait sur un seul de ces quinze processus, les documents présentés dans notre ouvrage nécessiteraient évidemment une réflexion complémentaire afin de détailler les étapes jalonnant le processus.

Mode d'utilisation des référentiels

Les deux approches (« globale » et « détaillée ») ne s'excluent pas l'une l'autre mais se complètent. Les référentiels proposés ici sont une base de travail pour l'auditeur interne.

Ils n'ont pas la prétention, malgré une volonté de précision et d'exhaustivité, de couvrir toutes les complexités et spécificités de toutes les organisations existantes.

En d'autres termes, l'auditeur devra à partir de ces documents :

- les compléter afin de tenir compte du contexte audité ;
- les enrichir, mission après mission, en fonction de l'expérience acquise, pour qu'ils constituent et conservent le savoir-faire du service d'audit interne ;
- et avant tout les confronter à la réalité de leur mise en œuvre.

APPROCHE GLOBALE

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
A. LES PRÉALABLES AU CONTRÔLE INTERNE					
A.1. Définition, déclinaison et communication des objectifs de l'organisation <i>*Définition des objectifs</i>	<ul style="list-style-type: none">Être sûr que les objectifs généraux de l'organisation sont connus, communiqués et déclinés avec précision au niveau de chaque responsable concerné (entités décentralisées, services...). Objectifs généraux déclinés en objectifs opérationnels, par un chiffre associé à une mesure de temps.	<ul style="list-style-type: none">Objectifs mal définis, imprécis ou impossibles à mesurer.Communication anarchique et irrégulière des objectifs.Imprécision de la déclinaison des objectifs.Incohérence des objectifs avec l'activité ou d'autres objectifs.Incohérence entre objectifs et moyens.Excès ou insuffisance de communication sur les objectifs.Nombre d'objectifs trop important ou insuffisant.Concertation insuffisante lors de la fixation des objectifs entraînant une non- adhésion des responsables concernés.	<ul style="list-style-type: none">Indicateurs correspondant aux objectifs.Fiches d'objectifs/ tableaux de bord.Fréquence des réunions de suivi et d'information.Synthèse des réunions entre la direction et les responsables concernés.Présences aux réunions des responsables concernés.	<ul style="list-style-type: none">Non-atteinte des objectifs.Mauvaise interprétation de la stratégie.Manque de cohérence avec la politique générale.Manque de mobilisation du personnel.Pertes financières/ productivité.Performances du service revues à la baisse.Décisions prises incohérentes avec les objectifs.Entité décentralisée qui ne suit pas les directives de la maison mère.Perte de crédibilité de la direction générale.	<ul style="list-style-type: none">Définir des objectifs quantifiés (à chaque objectif sont associés un ou plusieurs indicateurs et une mesure de temps).Diffuser les objectifs aux responsables de services concernés et aux collaborateurs.Mettre à jour et suivre régulièrement les objectifs.Formaliser et justifier l'atteinte des objectifs dans les entretiens de performance.Mettre en place un contrôle de gestion adapté.Faire participer les collaborateurs de l'organisation à la définition des objectifs avec les responsables de services afin d'en assurer la bonne réalisation.Formaliser de manière exhaustive les objectifs confiés aux collaborateurs.Organiser régulièrement des réunions de suivi des objectifs.Donner aux entités décentralisées les moyens de commenter les résultats et d'expliquer les difficultés d'atteinte des objectifs.

L'APPROCHE GLOBALE suivant le référentiel « AMF »(avec correspondance COSO)				
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES		EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	
A. LES PRÉALABLES AU CONTRÔLE INTERNE				
A.2. Règles d'exemplarité et d'intégrité <i>*Environnement de contrôle</i>	<ul style="list-style-type: none">– Être sûr de la formalisation, de la communication et du respect de l'ensemble des règles de conduite, d'intégrité et de culture d'entreprise au sein de l'organisation.	<ul style="list-style-type: none">– Absence de formalisation des « règles d'exemplarité et d'intégrité ».– Absence de communication de ces règles.– Incohérence de ces règles avec les actions et valeurs de la société.– Règles non appliquées par certains dirigeants (absence du principe d'exemplarité).	<ul style="list-style-type: none">– Charte éthique.– Code de bonne conduite.– Règlement intérieur.– Procédures de diffusion des documents à destination du personnel.– Modalités de communication des rémunérations dont celles des dirigeants (si le principe a été adopté).– Dispositif de <i>whistleblowing</i> (lanceur d'alerte) conformément à la loi Sapin 2.	<ul style="list-style-type: none">– Conflits d'intérêts.– Manque de cohérence avec la politique générale.– Perte d'esprit de groupe, d'esprit d'entreprise.– Risque d'absence de déontologie de la part des dirigeants ou des salariés.– Perte de crédibilité des instances dirigeantes de l'entreprise ; création de « pouvoirs parallèles ».– Risque d'image pouvant impacter la société.
				<ul style="list-style-type: none">– Définir, au plus haut niveau de l'organisation, un cadre général des principes éthiques (charte, code de conduite...).– Traduire ces concepts en principes d'actions collectives et individuelles déclinées vis-à-vis de chaque groupe de collaborateurs (ex. : « n'accepter aucun cadeau des fournisseurs pour les acheteurs »).– Porter à la connaissance de l'ensemble du personnel et des parties prenantes les règles de conduite (affichage, intranet...).– Organiser des campagnes de formation et sensibilisation à l'importance de la dimension éthique (<i>e-learning</i>).

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
A. LES PRÉALABLES AU CONTRÔLE INTERNE					
	<ul style="list-style-type: none">– Être sûr de la transparence dans la communication des informations.	<ul style="list-style-type: none">– Les règles sont mal définies ou mal interprétées.– Manque de transparence dans les prises de décision.	<ul style="list-style-type: none">– Définitions formalisées des responsabilités de chacun.– Procédure définissant les modalités de communication des rémunérations dont celles des dirigeants (si le principe a été adopté).– Rédacteurs des règlements et références légales identifiés.– Sanctions encourues en fonction de l'infraction clairement précisées.	<ul style="list-style-type: none">– Conflits d'intérêts.– Manque de légitimité envers les parties prenantes.– Perte d'esprit de groupe, d'esprit d'entreprise.– Risque d'absence de déontologie de la part des dirigeants ou des salariés.– Décisions inconnues des parties prenantes, empêchant l'application effective des règles.	<ul style="list-style-type: none">– Définir les principes éthiques de l'organisation (charte d'éthique).– Émettre des règlements clairement formalisés.– Mettre en place un service de communication ayant des objectifs définis en la matière.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
A. LES PRÉALABLES AU CONTRÔLE INTERNE					
A.3. « Règles du jeu » <i>*Environnement de contrôle</i>	– Être sûr que l'organisation dispose d'une connaissance suffisante des obligations (lois, réglementations...) qui s'imposent à elle (« règles du jeu »). L'information concernée doit être gérée : mise à jour, conservation, disponibilité, diffusion...	– Défaut de mise à jour des connaissances. – Défaut de diffusion des informations. – Absence de formation. – Diversité et densité des informations. – Les documents attestant de la conformité ne sont pas conservés ou sont égarés.	– Actions de formation du personnel. – Procédure de mise à jour des connaissances. – Procédure de veille sur les réglementations. – Procédure de diffusion des informations (planning, liste des destinataires, supports de diffusion...).	– Non-conformité aux obligations légales. – Litiges avec les employés. – Conflits avec les syndicats et les représentants du personnel. – Sanctions prud'homales. – Documents comptables erronés. – Environnement propice aux fraudes. – Risque d'image pouvant impacter la société.	– Sensibiliser et former le personnel aux obligations qui s'imposent à eux. – Mettre en place un dispositif de mise à jour des connaissances. – Mettre en place une procédure de veille sur les réglementations. – Mettre en place une procédure de diffusion des informations. – Mettre en place une procédure de conservation et d'archivage des documents attestant de la conformité de l'entité aux lois et réglementations en vigueur.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
B. ORGANISATION					
B.1. Organisation appropriée <i>*Environnement de contrôle</i>	<ul style="list-style-type: none">Être sûr que l'organisation est objective et adaptée à la culture d'entreprise, à l'environnement, au secteur d'activité et à la réalisation des objectifs.	<ul style="list-style-type: none">Périmètre de l'organisation non déterminé ou mal connu.Organes de gouvernance interne non définis.Absence de formalisation des liens entre les différents services.Taille de l'organisation inadaptée.Absence d'organigramme.Mauvaise estimation des ressources nécessaires à la réalisation des objectifs.Mauvaise appréhension de l'environnement de l'entreprise.Mauvaise connaissance de la culture de l'entreprise.	<ul style="list-style-type: none">Cartographie des processus.Organigramme.Grille de séparation des fonctions.Formalisation des pratiques et processus clés.Dispositifs de conservation du savoir-faire.Compte rendu des réunions des organes de gouvernance.Liste des pouvoirs.Liste des relations fonctionnelles.	<ul style="list-style-type: none">Remise en cause de la pérennité de l'entreprise.Dispositif de contrôle interne inadapté à l'organisation.Non-atteinte des objectifs.Manque de coordination.Mauvaise maîtrise des risques liés à l'activité.Perte de productivité.Pertes financières.Manque de fidélisation des collaborateurs.	<ul style="list-style-type: none">Déterminer le périmètre de l'organisation auquel s'applique le dispositif de contrôle interne.Définir les organes de gouvernance interne.Établir une cartographie des processus.Établir des procédures exhaustives, mises à jour et diffusées.Établir un organigramme.Définir clairement les postes et les activités de l'organisation.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
B. ORGANISATION					
	<ul style="list-style-type: none">Être sûr que l'organisation permet la réalisation des objectifs, ces derniers devant être planifiés, exécutés et contrôlés,	<ul style="list-style-type: none">Méconnaissance des objectifs.Périmètre de l'organisation non déterminé ou mal connu.Organes de gouvernance interne non définis.Mauvaise articulation des objectifs stratégiques et opérationnels.Non-adéquation entre les objectifs définis et les moyens mis à disposition pour les atteindre.	<ul style="list-style-type: none">Organes de gouvernance interne (comités d'audit, d'éthique...).Adéquation entre les besoins et les moyens mis à disposition, définition de politiques opérationnelles visant à l'atteinte des objectifs.Indicateurs de contrôle et plan d'actions.Plaquette de présentation de l'organisation, <i>business plan</i> et rapport annuel.Rapport de contrôle interne.	<ul style="list-style-type: none">Incohérence des actions avec les objectifs.Mauvaise circulation des informations.Mauvaise maîtrise des risques liés à l'activité.Perte de productivité.Pertes financières.Risque de démotivation du personnel.	<ul style="list-style-type: none">Organisation adaptée au secteur d'activité et à l'environnement.Mise à disposition des ressources matérielles, humaines et financières nécessaires afin d'atteindre les objectifs et de respecter la législation.Communication des objectifs de façon uniforme par le même canal de communication et depuis la même source.Définir le champ d'action de l'organisation : secteur d'activité, produits, clients, fournisseurs...

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF *Équivalences COSO	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
B. ORGANISATION					
B.2. Définition des responsabilités et des pouvoirs *Environnement de contrôle	– Être sûr que les responsabilités et pouvoirs sont attribués à des personnes appropriées selon les objectifs de l'organisation et en respectant le principe de séparation des fonctions.	– Organigramme inexistant, méconnu ou non respecté. – Absence d'arbitrage objectif lors des définitions de fonction.	– Organigramme. – Fiches de poste. – Délégations de pouvoir. – Liste des pouvoirs. – Fréquence des mises à jour. – Manuel des procédures.	– Perte de temps (méconnaissance des personnes habilitées, tâches doublons, tâches incompatibles). – Non-atteinte des objectifs. – Risque de fraudes. – Pertes financières. – Pertes de productivité. – Perte de crédibilité des supérieurs hiérarchiques.	– Définir un organigramme, des fiches de poste, une liste des personnes habilitées et des délégations de pouvoir avec la signature des personnes concernées. – Prévoir les accès aux fichiers/données en fonction des changements de situation du personnel (départs, entrées, promotions...).
	– Être sûr que ces responsabilités et pouvoirs sont formalisés et communiqués.	– Organigramme inexistant, méconnu ou non mis à jour. – Absence de répartition des tâches et des responsabilités (pas de liste de personnes habilitées, pas de fiches de poste). – Relation informelle.	– Organigramme. – Fiches de poste. – Liste des pouvoirs.	– Perte de temps (méconnaissance des personnes habilitées, tâches en doublon)... – Risque de cumul de fonctions incompatibles.	– Procédure de diffusion de ces documents à l'ensemble des personnes concernées. – Mise à jour régulière de ces documents.

L'APPROCHE GLOBALE suivant le référentiel « AMF »(avec correspondance COSO)					
Référentiel AMF *Équivalences COSO	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
B. ORGANISATION					
B.3. Politique et pratique de gestion des ressources humaines *Environnement de contrôle	<ul style="list-style-type: none">Être sûr que les services disposent de moyens humains suffisants (effectifs et compétences) à leur bon fonctionnement et à l'atteinte des objectifs fixés.	<ul style="list-style-type: none">Absence de définition d'une politique claire en matière de recrutement, de formation, de promotion, de rémunération, de fidélisation et de « bien-être au travail ».	<ul style="list-style-type: none">Dossiers individuels du personnel.Procédure de recrutement et de formation.Grille de rémunération.Contrats de travail.Bilans périodiques de compétence.Notes attribuées au personnel.	<ul style="list-style-type: none">Recrutement de personnes non compétentes.Personnel ne répondant pas aux attentes.Non-atteinte des objectifs.Performances revues à la baisse.Découragement et démotivation du personnel.Turnover important.	<ul style="list-style-type: none">Création des dossiers individuels du personnel contenant l'ensemble des documents nécessaires et/ou obligatoires.Mettre en place les procédures concernées (recrutement, formation...).Entretiens d'évaluation effectués par une personne habilitée.Plan de formation continue.Validation des besoins de recrutement.Grille pour les rémunérations et les promotions.Note de cadrage pour les rémunérations et les promotions.Gestion prévisionnelle des emplois et des compétences.
B.4. Système d'information (SI) *Information et communication	<ul style="list-style-type: none">Être sûr de l'adaptabilité du système d'information aux objectifs de l'organisation, de la conservation et la protection des données, de la continuité d'exploitation (procédures de secours).	<ul style="list-style-type: none">Système d'informations trop complexe ou insuffisant par rapport aux besoins du processus.Aucun plan de secours, de sécurité.Absence de formations du personnel à l'utilisation des systèmes d'information.	<ul style="list-style-type: none">Gestion des habilitations.Plan de secours, de continuité de l'exploitation, de sécurité.Programme de formation des utilisateurs.Études préalables des besoins.Guides d'utilisation des applications informatiques utilisées.	<ul style="list-style-type: none">Accès aux informations et données non sécurisés (fraudes).Système d'informations non adapté.Mise en danger de la continuité de l'exploitation.Risque de démotiver le personnel à utiliser convenablement le SI.	<ul style="list-style-type: none">Concevoir et gouverner le système d'information en fonction des besoins réels de l'organisation.Rendre opérationnel le système informatique (formation des utilisateurs, mise en place des infrastructures).Sécuriser l'accès aux données et programmes en fonctions des habilitations pour éviter les pertes d'informations.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
B. ORGANISATION					
B.5. Procédures, modes opératoires, outils et pratiques <i>*Environnement de contrôle</i>	<ul style="list-style-type: none">Être sûr que le dispositif de contrôle interne repose sur :<ul style="list-style-type: none">des procédures ou modes opératoires par action ou processus ;des outils ou instruments de travail ;des pratiques communément admises au sein de la société.	<ul style="list-style-type: none">Absence de référentiel de procédures.Procédures non mises à jour ou non communiquées.Formation insuffisante des collaborateurs.Procédures incomplètes et inefficaces.	<ul style="list-style-type: none">Cartographie des processus.Diffusion des informations.Manuel des procédures.Fréquence des mises à jour.Coherence globale de l'ensemble des procédures.Mise à disposition des modes opératoires, guides, procédures aux collaborateurs pour qu'ils puissent accomplir leur mission.Formalisation des procédures de CI au sein des services.	<ul style="list-style-type: none">Mauvaise exécution des tâches.Non-fiabilité des informations.Pertes financières.Possibilité de fraudes.Opérations non sécurisées.Perte de productivité, allongement des délais de traitement.Risques de conflits d'intérêts non arbitrés.Perte d'informations et de savoirs.Non-optimisation des pratiques.Découragement des salariés, baisse de leur engagement personnel.	<ul style="list-style-type: none">Définir les procédures, modes opératoires et outils nécessaires aux missions des collaborateurs.Formaliser les procédures de l'organisation et les diffuser de façon efficace.Veiller à ce que les modes opératoires, procédures ou autres documents soient connus et compris de tous.Veiller à la mise à jour des procédures et autres documents.Mettre en place une coordination des procédures de l'organisation.

L'APPROCHE GLOBALE suivant le référentiel « AMF »(avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
C. DIFFUSION EN INTERNE D'INFORMATIONS PERTINENTES					
C.1. Diffusion en interne d'informations pertinentes <i>*Information et communication</i>	<ul style="list-style-type: none">Être sûr que les circuits d'information (intranet, « papier »...) sont adaptés à la nature des informations transmises.	<ul style="list-style-type: none">Surplus d'informations :<ul style="list-style-type: none">essentiels parasitant les circuits d'information majeurs.Défaut d'information : des informations clés sont manquantes pour le bon fonctionnement de l'organisation.Non-respect des circuits d'information : présence de goulets de rétention d'information ou communications d'informations confidentielles à « la mauvaise cible ».	<ul style="list-style-type: none">Circuits d'information formalisés.Recensement de l'information afin de déterminer les destinataires appropriés.Processus de diffusion.Liste des informations prérequis pour le fonctionnement des fonctions clés.	<ul style="list-style-type: none">Informations transmises aux personnes inadéquates (absence de confidentialité de l'information).Non-atteinte des objectifs à cause d'un manque d'information.Retard au niveau de l'exploitation.Perte de productivité.Risque de démotivation du personnel « en manque » d'information.	<ul style="list-style-type: none">Transmettre les informations de manière synthétique pour les directions et plus détaillées pour l'exploitation.Formaliser un processus de diffusion avec liste sécurisée des personnes concernées.Recenser les informations nécessaires à la réalisation des objectifs et leur suivi.Mettre en place une sélection de l'information demandée en vue d'y apporter une réponse synthétique.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
C. DIFFUSION EN INTERNE D'INFORMATIONS PERTINENTES					
	<ul style="list-style-type: none">Être sûr que les informations sont fiables, pertinentes et qu'elles sont transmises aux personnes adéquates et disponibles en temps opportun.	<ul style="list-style-type: none">Communication déficiente, excès d'informations ou retard dans leur mise à jour et/ou leur diffusion.Protection et supports de l'information inadaptés.Absence d'étapes de validation dans le processus de communication de l'information.Non-respect de la confidentialité.	<ul style="list-style-type: none">Tableaux de bord.Supports de communication (affichage, intranet, courriers, notes de service...).Reporting.Liste des habilitations.Bilans sociaux (par exemple rapport RSE).Éléments statistiques utiles à la gestion.Délégations de responsabilité/supervision.Processus de diffusion.Politique de communication externe en cas de crise.Recensement de l'information afin de déterminer les destinataires appropriés.	<ul style="list-style-type: none">Objectifs non réalisés.Décisions de gestion prises sur des informations non fiables.Manque de réactivité, performances revues à la baisse.Mauvaise gestion de crise en cas d'incident.Informations transmises aux personnes inadéquates (absence de confidentialité de l'information).Non-fiabilité de l'information.Perte d'informations.Informations non exploitables car non exhaustives.	<ul style="list-style-type: none">Recenser et synthétiser les informations nécessaires à la réalisation des objectifs et leur suivi.S'assurer de la cohérence entre les catégories de destinataires et leur responsabilité.Gérer la diffusion des procédures (liste de destinataires, date d'application, délai de validité, procédures modifiées ou annulées...).Mettre en place un programme de priorisation des informations à traiter.La diffusion de l'information est déléguée de façon claire et supervisée à des individus identifiés.

L'APPROCHE GLOBALE suivant le référentiel « AMF »*(avec correspondance COSO)					
Référentiel AMF *Équivalences COSO	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
D. ANALYSE DE RISQUES					
D.1. Identification et recensement des risques *Identification des événements	<ul style="list-style-type: none">Être sûr que les principaux risques pouvant avoir un impact sur la capacité de l'organisation à atteindre ses objectifs sont identifiés et recensés de façon exhaustive.	<ul style="list-style-type: none">Clarification insuffisante des objectifs pénalisant l'identification des risques associés.Mauvaise appréhension des risques selon leur nature et leur impact.Domaine de définition des risques mal connu.Manque de moyens pour identifier les risques.	<ul style="list-style-type: none">Cartographie des risques.Manuel de procédures.Moyens alloués au recensement des risques.Existence et attributions d'une fonction <i>risk management</i>.	<ul style="list-style-type: none">Non-atteinte des objectifs de l'organisation.Mauvaise maîtrise des risques.Performance revue à la baisse et malversation (inefficacité, perte financière, fraude...).Risques importants non détectés.	<ul style="list-style-type: none">Mettre en place une cartographie des risques et un processus de recensement continu (mise à jour périodique).Cibler les risques par domaine : métiers, fonctions, catégories...Effectuer des entretiens individuels avec les managers des processus concernés.Créer une fonction <i>risk management</i> si nécessaire.
D.2. Évaluation des risques *Évaluation des risques	<ul style="list-style-type: none">Être sûr que les risques sont évalués de façon pertinente selon leur niveau d'impact et leur probabilité d'occurrence.	<ul style="list-style-type: none">Critères d'évaluation non définis ou imprécis.Critères d'évaluation des risques non pertinents.Sous-estimation de l'impact et/ou de la probabilité d'occurrence.Manque de moyens et d'outils pour évaluer les risques (occurrence et gravité des incidents).Manque de fiabilité de la cartographie des risques au niveau de leur nature (nouveaux risques liés aux nouvelles technologies par exemple).	<ul style="list-style-type: none">Fiches d'évaluations des risques répertoriant l'ensemble des critères.Statistiques d'occurrence et de la gravité des incidents rencontrés.Cartographie des risques.Hierarchisation des risques.Recensement des moyens mis en œuvre pour traiter les risques.	<ul style="list-style-type: none">Mauvaise maîtrise des risques.Performance revue à la baisse et malversation (inefficacité, perte financière, fraude...).Perte de temps.Pertes financières.Mauvaise identification et évaluation des risques.Risque sur- ou sous-évalué.	<ul style="list-style-type: none">Définir des critères d'évaluation des risques pertinents en fonction des objectifs et natures d'activité en tenant compte du degré d'occurrence et du niveau d'impact.L'évaluation des risques doit être complétée par un recensement des moyens mis en œuvre pour traiter ces risques et par l'identification des risques acceptés.Élaborer une cartographie des risques en tenant compte des fondamentaux de l'organisation avec une mise à jour périodique (apparitions de nouvelles menaces).Mettre à disposition des outils permettant d'évaluer les risques.Créer une fonction <i>risk management</i> si nécessaire.

L'APPROCHE GLOBALE suivant le référentiel « AMF »(avec correspondance COSO)					
Référentiel AMF *Équivalences COSO	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
D. ANALYSE DE RISQUES					
	– Être sûr d'avoir pris en compte l'environnement de l'organisation ainsi que les dispositifs de contrôle interne existants,	– Mauvaise appréciation de l'environnement de contrôle existant. – Absence d'investigations sur le terrain ou de reporting en provenance des entités décentralisées,	– Rapport de contrôle interne. – Reporting sur la situation financière et opérationnelle des entités décentralisées à différentes périodes. – Procédures de contrôle interne existantes,	– Mise en place d'un dispositif de contrôle inadapté. – Mauvaise appréciation des risques. – Manquement d'opportunités,	– Effectuer des démarches de <i>benchmarking</i> sur les évolutions du secteur. – Disposer d'une cartographie des dispositifs de contrôle interne pour l'ensemble des entités de l'organisation. – Créer une fonction « contrôle interne » si nécessaire.
D.3. Procédures de gestion des risques et surveillance *Traitement des risques	– Être sûr que les procédures de gestion et de surveillance des risques sont formalisées, connues et appliquées,	– Procédures absentes, imprécises ou non communiquées. – Responsabilités et rôles des personnes en charge de la gestion des risques et du suivi non définis ou imprécis. – Mauvaise communication entre les services d'audit interne et de <i>risk management</i> ,	– Procédure de gestion des risques. – Inventaires des risques survenus. – Fiches de mission des différents services et acteurs. – Organigramme,	– Incapacité à réagir en cas d'occurrence des risques. – Ralentissement de l'activité. – Non-atteinte des objectifs. – Performance revue à la baisse et malversation (inefficacité, perte financière, fraude...). – Superposition des dispositifs. – Non-maîtrise des impacts potentiels,	– Formaliser une procédure de gestion des risques précisant les différentes alternatives possibles dans le traitement du risque (évitement, recours à l'assurance, mise en œuvre d'un dispositif de contrôle interne...). – Définir de façon précise les rôles respectifs de l'audit interne, du <i>risk management</i> et du contrôle interne en la matière.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
E. SURVEILLANCE ET PILOTAGE					
E.1. Surveillance permanente et pilotage <i>*Suivi et pilotage du dispositif de contrôle interne</i>	<ul style="list-style-type: none">Être sûr que le dispositif de contrôle interne (DCI) est adapté à l'organisation et qu'il est piloté par une structure identifiée (fonction « contrôle interne » lorsqu'elle existe).	<ul style="list-style-type: none">Absence de structure de contrôle interne formalisée.DCI trop lourd : sur-contrôle.DCI insuffisant : le DCI ne couvre pas l'ensemble de l'organisation.Le positionnement de la fonction « contrôle interne » n'est pas précis.Le DCI s'avère inadapté compte tenu des objectifs et de l'organisation.	<ul style="list-style-type: none">Rapport sur le contrôle interne/plan stratégique de l'entreprise.Tableau de bord du DCI.Périmètre du DCI.Objectifs de la fonction « contrôle interne ».Organigramme et définitions de fonction des contrôleurs internes.	<ul style="list-style-type: none">Perte de productivité due à un gaspillage de ressources dans les opérations de contrôle.Des risques ne sont pas identifiés pouvant mettre en péril l'atteinte des objectifs.Non-atteinte des objectifs.Absence de crédibilité du management entraînant un désintérêt des collaborateurs au niveau du contrôle interne.	<ul style="list-style-type: none">Instaurer une structure dédiée à la surveillance permanente (recrutement, formation, reporting...).Mise à jour des procédures de CI.Impliquer tous les échelons hiérarchiques de l'organisation dans la tenue du DCI.Adapter le DCI et la nature des contrôles en fonction du secteur d'activité et des objectifs : « l'organisation ne vit pas pour le contrôle ».Positionner la fonction « contrôle interne » de façon claire dans l'organisation.Définir son rôle dans l'organisation et les objectifs à atteindre.

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF *équivalences COSO	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
E. SURVEILLANCE ET PILOTAGE					
	<ul style="list-style-type: none">– Être sûr que le dispositif de contrôle interne fait l'objet d'une surveillance permanente (pertinence et adéquation aux objectifs de l'organisation).	<ul style="list-style-type: none">– DCI inadapté ou inefficace.– Absence d'outil de surveillance permanente.– Manque de cohérence entre le DCI et les objectifs.– Absence de processus de supervision.– Absence d'encadrement.– Absence, difficulté de positionnement de l'équipe de contrôle interne.	<ul style="list-style-type: none">– Tableaux de bord.– Rapport sur la situation du contrôle interne.– Rapport sur les revues périodiques.– Tableau de bord de suivi des risques.– Certification du rapport de contrôle interne par les CAC.	<ul style="list-style-type: none">– Objectifs de l'entreprise non atteints.– Vision à court terme et non-anticipation des incidents.– Décisions prises non pertinentes.– Pérennité remise en cause.– Système budgétaire incohérent.– Non-réalisation et non-optimisation des opérations.– Non-fiabilité des informations.– Non-respect des réglementations.– Mauvaise supervision et évaluation du personnel.	<ul style="list-style-type: none">– Instaurer une structure dédiée à la surveillance permanente (recrutement, formation, reporting...).– Utiliser des outils tels que tableaux de bord de pilotage de contrôle interne.– Rédiger un rapport sur la situation du contrôle interne de l'entreprise.– Mise à jour des procédures de CI.– Mettre en place un dispositif d'autoévaluation du CI et des risques.– Utilisation d'outils de surveillance.– Évaluer le management (responsable de la qualité du contrôle interne).– Intégration d'indicateurs dans le tableau de bord du « président ».

L'APPROCHE GLOBALE suivant le référentiel « AMF » (avec correspondance COSO)					
Référentiel AMF <i>*Équivalences COSO</i>	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
E. SURVEILLANCE ET PILOTAGE					
E.2. Surveillance périodique <i>*Suivi et pilotage du dispositif de contrôle interne</i>	<ul style="list-style-type: none">Être sûr que le dispositif de contrôle interne fait l'objet d'une surveillance périodique afin d'identifier les défaillances et de proposer des actions de progrès.	<ul style="list-style-type: none">Acteurs du dispositif de surveillance périodique (CI, auditeurs internes AI, qualité...) non indépendants et/ou non objectifs.Critères d'évaluation non fiables, non pertinents.Absence d'archivage des contrôles effectués.Acteurs ne disposant pas des compétences requises.Inadéquation du niveau technique des auditeurs internes.Champ des activités de l'audit interne inapproprié.	<ul style="list-style-type: none">Rapports d'audit (interne et externe).Charte d'audit interne et du commissariat aux comptes (CAC).Programme annuel d'audit.Ordres du jour et comptes rendus des comités d'audit.Programme qualité de l'audit interne.Plan d'orientation sur les risques les plus importants.	<ul style="list-style-type: none">Décisions prises sur des informations non fiables (informations erronées car absence de double contrôle).Non-optimisation et non-conformité des opérations.Non-atteinte des objectifs.Non-réalisation des opérations.Non-respect des réglementations.Risque de fraudes.Perte de crédibilité de l'audit interne car les résultats de ses travaux ne représentent pas la réalité.	<ul style="list-style-type: none">Rédiger et faire valider par la direction générale et le conseil une charte d'audit interne qui définit ses missions, pouvoirs et responsabilités.Planifier des contrôles indépendants en fonction des risques recensés.Coordonner les activités de l'AI avec celles des CAC.Archiver l'ensemble des rapports d'audit de façon à être consulté à temps opportun.Rattacher le service d'audit interne directement à la direction générale et lui faire rendre compte au conseil (son émanation : le comité d'audit).S'assurer de l'indépendance de l'audit interne.Surveiller et évaluer l'efficacité du programme qualité de l'audit interne.

L'APPROCHE GLOBALE suivant le référentiel « AMF »(avec correspondance COSO)					
Référentiel AMF *Équivalences COSO	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
E. SURVEILLANCE ET PILOTAGE					
E.3. Information au conseil <i>*Information et communication</i>	<ul style="list-style-type: none">Être sûr que la direction générale rend compte de façon réelle et pertinente au conseil (ou comité d'audit) des caractéristiques essentielles du dispositif de contrôle interne et de management des risques.	<ul style="list-style-type: none">Structure de gouvernance inadaptée en matière de contrôle interne et de management des risques.Rôle du conseil (comité d'audit) imprécis.Multiplicité ou insuffisance des informations jugées essentielles.Retard dans la transmission des rapports/informations.Mauvaise interprétation des rapports d'audit.Planification et communication imprécises quant aux réunions du conseil.Remontée d'informations erronées, incomplètes.Département d'audit interne non indépendant.	<ul style="list-style-type: none">Rapports d'audit.Planning des comités d'audit.Ordres du jour et procès-verbaux des réunions.Documents de suivi.Rapports sur le contrôle interne.Reporting, tableaux de bord.Rapport annuel sur les travaux du comité d'audit.	<ul style="list-style-type: none">Obligations réglementaires non remplies.Prise de décisions erronées (manque d'informations essentielles, pertinentes).Recommandations et plans d'actions émis à la suite de ces réunions ne reflétant pas la réalité.Non-information du conseil.Engagement de la responsabilité de la direction générale.Perte de crédibilité du service d'audit interne.	<ul style="list-style-type: none">Mettre en place un comité d'audit et définir son rôle en matière de contrôle interne et de management des risques.Communiquer son planning des réunions.Définir le rôle de la direction générale et de l'audit interne (et autres instances de « contrôle ») en matière de contrôle interne et de management des risques dans le cadre du comité d'audit.Définir la périodicité de collecte et de transmission des informations nécessaires aux réunions du conseil.Contrôler la fiabilité des informations remises au conseil.

APPROCHE PAR PROCESSUS OU DOMAINES DE GESTION

- management – direction générale [p. 241](#)
- gestion des ressources humaines [p. 244](#)
- finance – comptabilité [p. 251](#)
- juridique – fiscal [p. 259](#)
- contrôle de gestion – reporting [p. 266](#)
- systèmes d'information [p. 274](#)
- recherche et développement [p. 279](#)
- marketing [p. 283](#)
- achats [p. 291](#)
- gestion des stocks [p. 297](#)
- production et services connexes [p. 302](#)
- commercial [p. 314](#)
- service après-vente [p. 328](#)
- logistique [p. 334](#)
- qualité – sécurité – environnement [p. 342](#)

Rappel : l'ensemble des référentiels présentés illustrent la dimension « activités de contrôles » commune aux deux modèles COSO et « AMF ».

Ils doivent être considérés comme le fruit d'un travail de recherche universitaire et nécessitent une adaptation au contexte de chaque organisation audité. Ces exemples de référentiels de risques pourront guider l'auditeur interne lors de l'élaboration des tableaux des risques, dans le cadre de leur mission globale d'« audit de filiales ».

PROCESSUS ET/OU DOMAINE : management – direction générale					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
1. Planifier	<ul style="list-style-type: none">Être sûr que pour toutes les activités prévues, les moyens matériels, financiers et humains sont déterminés et sont en adéquation avec les objectifs de l'organisation.	<ul style="list-style-type: none">Mauvaise identification des activités, des moyens et des responsabilités.Absence de calendrier d'exécution des activités.Outil de suivi inexistant.	<ul style="list-style-type: none">Tableau de planification.Liste des activités.Calendrier d'exécution des activités.Budget.Liste des responsabilités.	<ul style="list-style-type: none">Non-atteinte des objectifs.Impossibilité de suivre la réalisation des activités.Défaillances dans la structure entraînant une diminution de l'efficacité et l'efficacité de l'organisation.Mauvaise optimisation des ressources.Turnover important entraînant des besoins en formation et retardant ainsi la réalisation des opérations.	<ul style="list-style-type: none">Fixer les objectifs.Recenser l'ensemble des ressources dont dispose l'organisation (ressources humaines, matérielles et financières).Établir un planning pour la réalisation de chaque objectif qui sera communiqué à l'ensemble des managers.Définir dans ce planning des étapes permettant de s'assurer que l'atteinte des objectifs initiaux est toujours réalisable.Anticiper le renouvellement des équipes.
2. Piloter	<ul style="list-style-type: none">Être sûr d'une remontée d'information permettant d'apprécier le déroulement des activités et de prendre les décisions adéquates.	<ul style="list-style-type: none">Absence de dispositif de remontée de l'information.Non-fiabilité de l'information.Pas d'indicateur de mesure de la performance.Information trop tardive.	<ul style="list-style-type: none">Entretiens avec la direction générale.Choix des indicateurs pertinents.Comptes rendus de réunion entre la DG et les managers des différents services.Présence des managers concernés aux réunions de pilotage.	<ul style="list-style-type: none">Mauvaise appréciation de l'activité.Pérennité de l'entreprise.Non-atteinte des objectifs.Perte de temps dans la prise de décision.	<ul style="list-style-type: none">Définir un planning des réunions de pilotage entre la direction générale et les principaux responsables opérationnels et fonctionnels.Définir des modèles de tableaux de bord déclinés pour chaque responsable.Définir un calendrier institutionnel de diffusion des informations nécessaires au pilotage des activités.

PROCESSUS ET/OU DOMAINE : management – direction générale					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
3. Veiller à la sauvegarde des actifs de l'organisation	<ul style="list-style-type: none">Être sûr de la correcte protection des actifs de l'entreprise.	<ul style="list-style-type: none">Absence de recensement des actifs significatif de l'organisation.Sous-estimation des actifs immatériels.	<ul style="list-style-type: none">Contrat d'assurance.Procédure de déclaration des sinistres.Procédure de revue périodique des contrats d'assurance.Procédure de protection de la propriété intellectuelle de l'organisation.Procédure de suivi des remboursements des sinistres.	<ul style="list-style-type: none">Actifs mal protégés, risque de perte financière.Litige avec la compagnie d'assurance.Surévaluation de la prime d'assurance.Risque de vol.Risque de perte du savoir de l'organisation.	<ul style="list-style-type: none">Existence de moyens de protection des actifs matériels (contre le vol, l'incendie...).Procédure de dépôt de brevets.Contrat d'assurance réévalué en fonction de l'évolution de l'organisation.Déclaration rapide des sinistres selon une procédure précise et connue de tous.Suivi du remboursement des sinistres.
4. Contrôler et analyser les résultats financiers	<ul style="list-style-type: none">Être sûr que les résultats financiers sont périodiquement comparés aux objectifs initiaux.	<ul style="list-style-type: none">Les données de sorties ne sont pas fiables.Le système d'information (SI) est mal paramétré.Pas de réunion d'analyse des résultats au niveau de l'organisation (direction générale et principaux responsables).Mauvaise déclinaison des objectifs par services.Le SI ne permet pas de produire des tableaux de bord de suivi.	<ul style="list-style-type: none">Système d'information.Planning des réunions d'analyse des résultats.Formalisation des objectifs généraux et de leur déclinaison en objectifs par processus et/ou fonctions.Organigramme et définitions de fonction.Indicateurs mis à disposition du management.	<ul style="list-style-type: none">Absence d'information pour piloter l'organisation.Difficulté pour les prises de décisions erronées.Difficulté et/ou erreur lors de la consolidation des résultats.Pas de valorisation du travail des collaborateurs.	<ul style="list-style-type: none">Définir une procédure précisant les modalités d'analyse des résultats financiers (périodicité, informations nécessaires, personnes concernées...).Définitions de fonction intégrant cette responsabilité pour les personnes concernées.Existence de tableaux de bord pertinents.Formalisation d'une pratique budgétaire (établissement et suivi des budgets).Existence d'une fonction contrôle de gestion indépendante.Existence de réunions périodiques réunissant la direction générale et les principaux responsables afin de rendre compte de l'atteinte des objectifs et ainsi favoriser la transmission régulière de l'information.

PROCESSUS ET/OU DOMAINE : management – direction générale					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
5. Communiquer les résultats à la maison mère (cas d'une filiale)	<ul style="list-style-type: none">– Être sûr de l'existence et du respect des procédures de remontée des informations de la filiale à la maison mère (reporting).	<ul style="list-style-type: none">– Absence de reporting.– Absence de procédure détaillée.– Procédure non appliquée.– Le SI de la filiale ne permet pas d'alimenter le reporting établi et destiné à la maison mère.– Les données ne sont pas fiables.– Absence de planning des remontées d'informations.	<ul style="list-style-type: none">– Procédure sur les remontées d'informations à la maison mère.– Caractéristiques du système d'information (SI) quant à sa capacité à alimenter le reporting de la maison mère.– Planning du reporting.– Entretiens avec le service « consolidation » de la maison mère.	<ul style="list-style-type: none">– Manque de réactivité sur le suivi de la réalisation des objectifs par la maison mère.– Erreur dans la stratégie locale et globale.– Manque de coordination engendrant une faiblesse face à la concurrence.– Pas de vision à moyen long terme.	<ul style="list-style-type: none">– SI de la filiale intégrant les exigences du reporting à la maison mère.– Formalisation d'une procédure précisant les modalités du reporting (planning, nature des informations demandées, responsables concernés en filiales et au niveau du groupe,...).

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. RECRUTEMENT ET ÉVOLUTION DE CARRIÈRE					
A.1. Identification du besoin de recrutement	<ul style="list-style-type: none">– Être sûr que le besoin de recrutement est correctement formalisé et communiqué.– Être sûr que le recrutement se fait notamment en fonction de l'évolution des compétences, des métiers, de l'anticipation des départs et/ou mutations.	<ul style="list-style-type: none">– Absence de formalisation des besoins en recrutement de la part des services demandeurs.– Mauvaise formalisation de ces besoins (pas de fiche précisant le profil du poste recherché).– Absence de communication efficace de ces besoins.– Mauvaise connaissance des besoins en personnel liée aux changements de l'organisation.	<ul style="list-style-type: none">– Procédure de recrutement.– Fiches de profils des postes recherchés et description des critères d'embauche.– Entretiens avec les responsables des différents services demandeurs.– Étude prévisionnelle du marché du secteur.	<ul style="list-style-type: none">– Absence de recrutement.– Recrutement inapproprié.– Pertes financières.– Baisse de la productivité.– Non-atteinte des objectifs.– Être en sous-effectif et/ou ne pas disposer des compétences adéquates.	<ul style="list-style-type: none">– Formaliser par écrit la procédure de recrutement intégrant toutes les étapes (expression du besoin, rôles et responsabilités des acteurs, méthodes de sélection...).– Rédaction de fiches « Profil de poste ».– Entretiens réguliers avec les différents services.

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. RECRUTEMENT ET ÉVOLUTION DE CARRIÈRE					
A.2. Recrutement du personnel	<ul style="list-style-type: none">– Être sûr que le personnel recruté correspond aux besoins de l'organisation (effectifs et compétences).	<ul style="list-style-type: none">– Difficulté et/ou incapacité à sélectionner les bons profils correspondant aux exigences des postes à pourvoir.– Manque d'attractivité de l'organisation sur le marché de l'emploi.– Mauvaise formalisation des besoins (pas de fiche précisant le profil du poste recherché).– Manque de candidats qualifiés.	<ul style="list-style-type: none">– Procédure de recrutement existante.– Fiches « Profil de poste » et description des critères d'embauche.– Entretiens avec les responsables des différents services demandeurs.– Étude prévisionnelle du marché du secteur.	<ul style="list-style-type: none">– Personnel sur- ou sous-qualifié.– Sur- ou sous-effectif.– Pertes financières.– Baisse de la productivité.– Mécontentement du personnel.– Non-atteinte des objectifs.– Perte du savoir-faire.	<ul style="list-style-type: none">– Formaliser par écrit la procédure de recrutement intégrant toutes les étapes (expression du besoin, rôles et responsabilités des acteurs, méthodes de sélection...).– Favoriser la promotion interne avant de procéder aux sélections de candidats en externe.– Mettre à jour régulièrement l'analyse des besoins prévisionnels en termes d'effectifs, dans le cadre de la planification des activités.– Mettre en place un dispositif de suivi des nouveaux embauchés durant la période d'essai afin de valider de façon pertinente leur contrat.– Développer des outils de communication afin de rendre la société attractive sur le marché de l'emploi.

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. RECRUTEMENT ET ÉVOLUTION DE CARRIÈRE					
A.3. Plan de carrière, mutations et promotions	<ul style="list-style-type: none">Être sûr que les aspirations des salariés de l'organisation sont prises en compte dans le cadre d'une politique d'évolution des carrières.	<ul style="list-style-type: none">Absence d'une politique d'évolution des carrières.Absence de communication sur les postes à pourvoir en interne.Absence de politique en matière de reconnaissance des « talents ».	<ul style="list-style-type: none">Procédure interne de promotion.Questionnaire de satisfaction des salariés sur leur possibilité d'évolution.	<ul style="list-style-type: none">Manque d'implication.Manque de motivation.	<ul style="list-style-type: none">Mise en place d'une gestion prévisionnelle des compétences.Mise en place d'une communication interne pour informer les salariés sur les postes à pourvoir.Définition d'une politique en matière de reconnaissance des « talents ».
A.4. Analyse des postes et évaluation des personnes	<ul style="list-style-type: none">Être sûr que les postes existants sont pertinents.	<ul style="list-style-type: none">Fonctions et postes ne faisant pas l'objet d'une définition claire.Absence de veille sur les évolutions de postes et de fonctions.	<ul style="list-style-type: none">Document type d'analyse de poste.Fiches de définition de fonction.	<ul style="list-style-type: none">Manque de cohésion, de transparence entre les postes.Existence de postes inutiles.Perte financière et perte de performance.	<ul style="list-style-type: none">Mise en place de documents types permettant de faire le point sur les postes.Veille des compétences.
A.5. Évaluation des personnes	<ul style="list-style-type: none">Être sûr que les salariés sont évalués objectivement et régulièrement.	<ul style="list-style-type: none">Pas de fiche type d'évaluation des salariés.Pas de procédure d'évaluation des compétences.Pas de communication des résultats d'évaluation aux personnes concernées.	<ul style="list-style-type: none">Comptes rendus d'entretien annuel d'évaluation.Procédure existante d'évaluation des personnes.	<ul style="list-style-type: none">Démotivation des salariés.Risque de poursuite juridique.Promotion des « mauvaises » personnes aux « mauvais » postes.	<ul style="list-style-type: none">Mise en place d'un guide d'entretien individuel d'évaluation.Établissement de bilan de compétences.Grille d'auto-évaluation.Communication des résultats aux personnes concernées.

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. RECRUTEMENT ET ÉVOLUTION DE CARRIÈRE					
A.6. Rotation du personnel	<ul style="list-style-type: none">Être sûr que la rotation du personnel est à un niveau pertinent (turnover et rotation nécessaire des postes maîtrisés).	<ul style="list-style-type: none">Les rémunérations et avantages proposés par l'organisation ne sont pas concurrentiels.Les salariés peuvent avoir le sentiment que leurs efforts ne sont pas reconnus.Les salariés sont réfractaires à la mobilité professionnelle.	<ul style="list-style-type: none">Taux de turnover.Grille de salaires de référence.Fiches d'évaluation du personnel.Existence de réunion permettant une remontée d'informations sur la satisfaction des salariés.	<ul style="list-style-type: none">Démotivation du personnel.Turnover important.Départ des meilleurs éléments.Installation de certaines catégories de salariés dans une routine professionnelle.	<ul style="list-style-type: none">Disposer d'une véritable politique en matière de plan de carrière.Mettre en place un <i>benchmark</i> concernant les salaires et avantages proposés par les autres organisations du même secteur d'activité.Étude et évaluation régulière des rémunérations et avantages accordés par l'organisation.Formaliser les facteurs d'évolutions de la rémunération.
B. RÉMUNÉRATION					
B.1. Salaire et son évolution	<ul style="list-style-type: none">Être sûr que les rémunérations sont conformes à la législation et/ou à la convention collective.	<ul style="list-style-type: none">Grille de salaires non conforme.Pas de personne responsable des mises à jour.Absence de politique salariale.	<ul style="list-style-type: none">Grille de salaires.Conventions collectives.Dispositions législatives en matière de rémunération.	<ul style="list-style-type: none">Non-respect de la législation ou des conventions collectives.Risque de fraude (baisse des cotisations sociales).Démotivation du personnel.Turnover important.	<ul style="list-style-type: none">Définir une politique salariale conforme aux conventions collectives et aux dispositions législatives.Mettre en place une veille réglementaire en la matière.

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
B. RÉMUNÉRATION					
	<ul style="list-style-type: none">Être sûr qu'il y a adéquation, pour chaque catégorie de postes, entre les compétences requises et le niveau de qualification des salariés (diplôme, expérience...).	<ul style="list-style-type: none">Pas de personne responsable des mises à jour.Absence de nomenclature des postes et de grille de salaires.Absence d'arbitrage lors de l'attribution des postes.	<ul style="list-style-type: none">Définitions de fonction.Liste des qualifications requises par catégorie de postes.Dossiers du personnel.Grille de salaires en fonction du niveau de qualification.	<ul style="list-style-type: none">Insatisfaction des salariés.Absence des compétences requises au poste donné.Démotivation des candidats ou des nouveaux embauchés.	<ul style="list-style-type: none">Mise en œuvre d'une gestion des dossiers individuels du personnel (qualification lors de l'embauche, formations suivies, expériences acquises...).Définir une politique salariale conforme aux conventions collectives et aux dispositions législatives.
B. 2. Autres éléments de rémunération	<ul style="list-style-type: none">Être sûr que l'organisation respecte ses engagements vis-à-vis de ses salariés concernant les « autres éléments de rémunération » (participation et intéressement, primes, avantages divers...).	<ul style="list-style-type: none">Méconnaissance des engagements en la matière.Absence et/ou faiblesse du système d'information permettant de transmettre au service concerné les justificatifs de ces primes et avantages divers.Retard dans le règlement des montants concernés.	<ul style="list-style-type: none">Distribution effective de la participation, de l'intéressement, des primes...Calcul effectif des montants.Dossiers du personnel.Entretien avec les responsables du comité d'entreprise et autres instances représentatives.	<ul style="list-style-type: none">Risques de conflits sociaux.Poursuites prud'homales, impliquant pertes financières.Insatisfaction du personnel.Démotion des cadres.	<ul style="list-style-type: none">Formaliser tous ces éléments de rémunération (hors salaire) dans les dossiers individuels du personnel.Définir une procédure de calcul et de versement de la participation et de l'intéressement.Versement des primes aux salariés suivant les critères et la périodicité convenus.

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
C. FORMATION					
C. 1. Détection des besoins et élaboration du plan de formation	<ul style="list-style-type: none">Être sûr que chaque salarié peut bénéficier des formations lui convenant et correspondant aux besoins de l'organisation.	<ul style="list-style-type: none">Absence de préoccupation en la matière.Absence de démarches pour connaître les besoins en formation.Choix subjectifs concernant les personnes à former et les domaines objet de la formation.	<ul style="list-style-type: none">Pratiques concernant l'identification des besoins en matière de formation : plan de formation, cahier des charges, fiches formation...Circuit de validation d'une formation.	<ul style="list-style-type: none">Manque de compétences.Pas d'évolution possible des carrières et des connaissances de certains salariés.Manque d'implication des salariés.Perte de compétitivité.	<ul style="list-style-type: none">Établir des fiches types pour connaître les besoins et les attentes de chacun.Entrettenir une relation client/fournisseur entre le service formation et les clients internes.Sensibiliser chaque responsable de service à la nécessité et l'importance de la formation.
	<ul style="list-style-type: none">Être sûr que l'organisation respecte ses obligations en matière de formation.	<ul style="list-style-type: none">Méconnaissance des obligations en la matière.Budget insuffisant.	<ul style="list-style-type: none">Obligations en matière de formation.Plan de formation.Attestations des formations réalisées.	<ul style="list-style-type: none">Manque de compétences des salariés.Pas d'évolution possible des carrières et des connaissances de chacun.Manque d'implication des salariés.Perte de compétitivité.	<ul style="list-style-type: none">Mettre en place une veille réglementaire.Définir une politique claire (formation en interne ou en externe, individuelle ou collective, avec des objectifs à atteindre).Atribuer un poste de responsable formation et créer des indicateurs de performance pour cette fonction.

PROCESSUS ET/OU DOMAINE : gestion des ressources humaines					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE					
(découpage du processus et/ou domaine de gestion)					
C. FORMATION					
C. 2. Mise en œuvre des actions de formation	<ul style="list-style-type: none">Être sûr que les formations sont réalisées conformément aux cahiers des charges.	<ul style="list-style-type: none">Manque de compétences chez les formateurs.Formations inadaptées (contenu et niveau ne correspondant pas aux attentes et besoins des stagiaires).	<ul style="list-style-type: none">Entretiens avec le service formation.Cursus antérieur à chaque formateur.Cahiers des charges des formations réalisées.	<ul style="list-style-type: none">Formations inefficaces.Démotivation des participants ressentant cela comme une perte de temps.	<ul style="list-style-type: none">Définir une procédure de mise en œuvre des formations.Mettre en place des formations pertinentes par rapport à l'activité et au métier.Effectuer la veille sur les évolutions des métiers de l'organisation.Vérifier les expériences antérieures des formateurs.
	<ul style="list-style-type: none">Être sûr que les formations sont correctement effectuées.	<ul style="list-style-type: none">Pas de fiche de présence.Pas de responsable, pas d'encadrement.Pas de correspondance entre la demande et la formation.Manque de compétences des formateurs.	<ul style="list-style-type: none">Documents relatifs aux formations (détails, planning de la journée, modalités).Vérifier que les salariés sont informés du déroulement de la formation (communication).	<ul style="list-style-type: none">Formations inefficaces.Démotivation des stagiaires ressentant cela comme une perte de temps.Gaspillage de ressources.	<ul style="list-style-type: none">Établir un document de déroulement de la formation.Communiquer toutes les informations concernant les formations aux stagiaires.Formaliser tous les supports de formation et veiller à ce qu'ils soient à jour.Vérifier les expériences antérieures des formateurs.
C. 3. Évaluation des résultats	<ul style="list-style-type: none">Être sûr de l'efficacité des formations et de la satisfaction des besoins et attentes des participants.	<ul style="list-style-type: none">Pas de dispositif d'évaluation de la formation ni par le stagiaire ni par sa hiérarchie.Pas de fiche de suivi durant la formation.Évaluation non objective.	<ul style="list-style-type: none">Documents de suivi.Procédures d'évaluation des résultats.Fiches synthèses des remarques des participants.	<ul style="list-style-type: none">Inadaptation des formations.Perte de crédibilité de la formation : apparition de formations « pirates ».Démotivation des stagiaires.	<ul style="list-style-type: none">Définir une procédure d'évaluation des formations (par les participants et par les responsables hiérarchiques des participants).Désigner une personne du service formation ne mettant pas en place les formations, chargée de la synthèse de ces évaluations.

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
1. Gestion des immobilisations/ amortissements	– Être sûr que les comptes d'immobilisations corporelles sont fiables (exactitude, exhaustivité).	– Absence d'inventaire régulier des immobilisations corporelles. – Certaines immobilisations ne sont pas comptabilisées. – Valorisation erronée des immobilisations.	– Compte rendu des inventaires des immobilisations. – Méthode de valorisation des immobilisations. – Séparation des fonctions entre la personne habilitée à provisionner et celle habilitée à saisir les écritures.	– États financiers erronés. – Détournements, fraudes. – Risque de non-certification des comptes. – Mauvaises décisions de gestion car prises sur la base d'informations fausses ou approximatives.	– Formalisation d'une procédure de suivi des immobilisations (entrée et sortie du patrimoine, inventaire, valorisation...). – Création d'une liste de personnes habilitées pour chaque type de mouvements comptables. – Réaliser des rapprochements périodiques entre le fichier des immobilisations et les comptes de classe 2 en comptabilité.
	– Être sûr que les opérations sur titres, l'attribution de prêts (notamment les prêts aux filiales...) sont correctement comptabilisées et font l'objet d'un suivi.	– Absence de procédure d'autorisation des opérations sur titres et d'attribution des prêts aux filiales. – Erreur sur le taux d'amortissement. – Erreur sur le mode d'amortissement.	– Liste des personnes habilitées à signer un bon de cession ou de mise aux rebus. – Procédure claire de cession des immobilisations.	– États financiers erronés. – Détournements, fraudes. – Risque de non-certification des comptes. – Mauvaises décisions de gestion car prises sur la base d'informations fausses ou approximatives.	– Référencement et suivi des prêts aux filiales. – Rapprochement des amortissements avec les prêts.

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">– Être sûr que les amortissements sont correctement calculés et comptabilisés,	<ul style="list-style-type: none">– Taux d'amortissement erroné.– Mode d'amortissement inadapté.– Les provisions sont surévaluées ou sous-évaluées.	<ul style="list-style-type: none">– Contrôler l'exactitude des provisions.– Séparation des fonctions efficace entre la personne habilitée à provisionner et celle habilitée à saisir les écritures.	<ul style="list-style-type: none">– États financiers erronés.– Détournements, fraudes.– Risques de non-certification des comptes.– Mauvaises décisions de gestion car prises sur la base d'informations fausses ou approximatives.	<ul style="list-style-type: none">– Contrôle des provisions.– Création d'une liste de personnes habilitées pour chaque type de mouvements comptables.– Mettre en place un référentiel concernant les différentes provisions à effectuer sur l'année et la manière dont cela doit être fait.– Réaliser des contrôles périodiques de cohérence entre les amortissements du fichier des immobilisations et ceux réellement comptabilisés en classe 2.
2. Comptes d'achats	<ul style="list-style-type: none">– Être sûr du suivi et du contrôle des comptes fournisseurs,	<ul style="list-style-type: none">– Absence ou mauvaise application des procédures de comptabilisation des achats.– Liberté dans la création de compte fournisseur.– Absence de séparation des fonctions.	<ul style="list-style-type: none">– Procédure de comptabilisation des factures fournisseurs.– Procédure de création de comptes fournisseurs.– Rapprochements bancaires.– Liste des habilitations comptables fournisseurs.	<ul style="list-style-type: none">– États financiers erronés.– Détournements, fraudes.– Mauvaises décisions de gestion car prises sur la base d'informations fausses ou approximatives.– Sur-paiement de certaines prestations et/ou fournitures.	<ul style="list-style-type: none">– Procédure claire et exhaustive de comptabilisation des factures fournisseurs.– Instaurer une séparation des fonctions, création de compte fournisseur, entrée des écritures et comptabilisation (personnes habilitées).– Vérification périodique des comptes fournisseurs (existence d'une balance âgée).

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
3. Comptes de produits	– Être sûr du suivi et du contrôle des comptes clients.	– Absence ou mauvaise application des procédures de comptabilisation des produits. – Manque de rigueur dans l'établissement des factures. – Liberté dans la création de comptes clients. – Absence de séparation des fonctions.	– Procédure de comptabilisation des factures clients. – Procédure de création de comptes clients – Rapprochements bancaires. – Liste des habilitations comptables clients.	– États financiers erronés. – Détournements, fraudes. – Mauvaises décisions de gestion car prises sur la base d'informations fausses ou approximatives.	– Existence d'une procédure claire et exhaustive de comptabilisation des factures clients. – Rapprochement entre les factures et les biens ou services effectivement livrés. – Vérifier que le service concerné s'est assuré de la solvabilité du client avant de créer son compte.
	– Être sûr du recouvrement des créances clients.	– Absence de préoccupation au niveau du recouvrement des créances clients. – Absence de directives précises.	– Système de relance des impayés. – Incidents survenus.	– États financiers erronés. – Pertes financières. – Procédure judiciaire.	– Mise en place d'une procédure d'appréciation de la solvabilité des clients. – Existence d'une balance âgée. – Mise en place d'une procédure de relance des impayés. – Suivi des dossiers clients.
4. Clôture des comptes	– Être sûr que les travaux comptables concernant la clôture des comptes sont planifiés.	– Absence ou non-application des procédures comptables. – Absence de responsable chargé de superviser l'application des règles comptables en matière de clôture des comptes.	– Planning des étapes concernant la clôture des comptes. – Situation sur les clôtures précédentes. – Procédure de consolidation.	– Retard dans la production des états financiers. – Non-certification des commissaires aux comptes (CAC).	– Mise en place d'un planning des travaux de clôture des comptes (désignation d'un responsable de la coordination).

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr de la bonne application des règles comptables, fiscales et juridiques lors de la clôture des comptes.	<ul style="list-style-type: none">Non-respect ou méconnaissance des règles comptables, fiscales et juridiques.Absence de responsable chargé de superviser l'application de ces règles.Application de plusieurs types de comptabilité au sein d'un même groupe.	<ul style="list-style-type: none">Principes, règles et procédures comptables.Rapports des commissaires aux comptes.Liste d'habilitation pour les arrêtés de compte et la consolidation.	<ul style="list-style-type: none">États financiers erronés.Impossibilité de connaître avec précision les performances de l'entreprise.Non-certification des commissaires aux comptes (CAC).	<ul style="list-style-type: none">Répertorier l'ensemble des obligations comptables, fiscales et juridiques qui s'imposent à l'organisation lors de la clôture des comptes.Désigner un responsable en charge de la bonne application de ces obligations.Définir pour l'organisation une norme comptable unique.
	<ul style="list-style-type: none">Être sûr que les éléments et flux comptabilisés se rattachent bien à l'exercice concerné.	<ul style="list-style-type: none">Intégration « anticipée » d'écritures dans l'exercice de l'année en cours.Report d'écritures de fin d'année sur l'exercice suivant.	<ul style="list-style-type: none">Dates des documents se rapportant aux écritures.Procédure de clôture d'exercice comptable.	<ul style="list-style-type: none">États financiers erronés.Non-certification des commissaires aux comptes (CAC).	<ul style="list-style-type: none">Répertorier l'ensemble des obligations comptables, fiscales et juridiques qui s'imposent à l'organisation lors de la clôture des comptes.Désigner un responsable en charge de la bonne application de ces obligations.Effectuer les rapprochements entre les écritures et les pièces comptables.
5. Trésorerie	<ul style="list-style-type: none">Être sûr de maîtriser au mieux les prévisions de trésorerie afin d'utiliser de la manière la plus efficiente possible les fonds à la disposition de l'entreprise.	<ul style="list-style-type: none">Les encaissements ou décaissements ne sont pas ou mal comptabilisés.Absence ou insuffisance de communication entre les services de l'organisation dont l'activité impacte les prévisions de trésorerie.Pas d'application informatique pour la gestion de trésorerie.	<ul style="list-style-type: none">Procédure de reporting financier exhaustive afin de baser les prévisions de façon optimale.Délégation de signatures et habilitations.Système d'approbation des décaissements.Consolidation des données de trésorerie.	<ul style="list-style-type: none">Utilisation de la trésorerie non optimale.Pertes financières.Risques de non-certification des comptes.	<ul style="list-style-type: none">Disposer d'une application informatique pour la gestion de la trésorerie.Établir des échéanciers précis afin d'identifier les dates prévisionnelles concernant les encaissements et décaissements.Consolider les informations de trésorerie avant toute prise de décision.Définir les habilitations pour tout décaissement.

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr de régler les fournisseurs, verser les salaires, rembourser les emprunts, payer les impôts et effectuer tous les autres décaissements suivant les échéances prévues.	<ul style="list-style-type: none">Méconnaissance par les services concernés des engagements de paiement pris.Règlements inexacts du fait d'une comptabilité approximative.	<ul style="list-style-type: none">Système de suivi des paiements fournisseurs.Alertes d'échéances de versement existant dans le SI.Délégations de signature.Système d'approbation des décaissements.	<ul style="list-style-type: none">Pertes financières.Paiements non effectués conformément aux engagements pris.	<ul style="list-style-type: none">Établir un échéancier clair afin d'identifier les dates de paiement.Vérifier la concordance des sommes à payer et les bénéficiaires avec les factures.S'assurer que la trésorerie est suffisante pour assurer les paiements.Comparer les sommes réellement payées à celles qui étaient prévues de l'être.
6. Paie	<ul style="list-style-type: none">Être sûr de l'exactitude de l'enregistrement des charges de personnel.	<ul style="list-style-type: none">Les conventions collectives ne sont pas appliquées ou pas connues.Méconnaissance des règles comptables en matière de salaires.Mauvais paramétrage de l'application informatique de traitement de la paie.	<ul style="list-style-type: none">Conventions collectives.Principes comptables en matière d'enregistrement des charges de personnel.Grille de rémunérations.	<ul style="list-style-type: none">Erreurs dans les salaires versés.Perte de motivation de la part des salariés.Maîtrise de la masse salariale non optimale.Image de la société affectée.	<ul style="list-style-type: none">Vérifier l'application des conventions collectives.Contrôler la bonne application des principes comptables.Identifier clairement un responsable de la paie.S'assurer du respect de la séparation des tâches en la matière et vérifier l'accès au logiciel de paie.S'assurer que le système d'alerte est en place pour identifier les incidents de versement (double paiement, montants erronés...).

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objec- tifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'em- pêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr de la cohérence de la politique salariale.	<ul style="list-style-type: none">Les conventions collectives ne sont pas appliquées ou pas connues.Des disparités existent au niveau de la paie en fonction des sites.La politique de rémunération n'est pas en phase avec les objectifs de l'organisation.Une partie de la paie est sous-traitée.Les rémunérations de certains dirigeants ne transitent pas par le circuit de la paie.	<ul style="list-style-type: none">Conventions collectives.Grille de rémunérations.Répartition de la paie entre chaque catégorie de salariés.En cas de sous-traitance partielle ou totale de la paie, rapport d'audit effectué chez le prestataire.	<ul style="list-style-type: none">Image de la société affectée.Rémunérations non équitables.Démotivation des salariés, risque de poursuites.Risque de conflit interne.	<ul style="list-style-type: none">Vérifier l'application des conventions collectives.S'assurer de la cohérence de la politique salariale (dans le temps et entre les catégories de salariés).Identifier clairement un responsable de la paie.Dans le cas d'une sous-traitance partielle ou totale du versement de la paie, effectuer des contrôles périodiques sur le prestataire.
7. Financement	<ul style="list-style-type: none">Être sûr que les meilleurs choix sont faits en matière de financement.	<ul style="list-style-type: none">Mauvaises prévisions financières.Manque de clarté dans la communication financière.	<ul style="list-style-type: none">Procédures existantes.Dossiers de financement récents et significatifs.	<ul style="list-style-type: none">Augmentation des charges financières.Le financement ne correspond pas au besoin.	<ul style="list-style-type: none">Formalisation d'une procédure précisant les modalités de financement (responsabilités, calcul des besoins, sélection du mode de financement...).
8. Caisse	<ul style="list-style-type: none">Être sûr qu'on vérifie les mouvements de caisse.	<ul style="list-style-type: none">Pas de procédure mise en place.Pas de supervision de la personne en charge de la tenue de la caisse.	<ul style="list-style-type: none">Vérifier l'existence d'une procédure.Liste des personnes habilitées.	<ul style="list-style-type: none">Erreur de caisse.Risque de fraude.	<ul style="list-style-type: none">Formalisation d'une procédure de tenue de la caisse (responsabilités, niveau de reconstitution, contrôles périodiques des pièces justificatives...).

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
9. Stocks	<ul style="list-style-type: none">Être sûr que tous les stocks sont correctement évalués et comptabilisés.	<ul style="list-style-type: none">Absence ou non-respect de la procédure établie pour les inventaires physiquesAucun suivi des stocks et/ou inventaire permanent défectueux.Méconnaissance des règles comptables (coûts unitaires, dépréciation...).	<ul style="list-style-type: none">Procédure d'inventaire physique.Inventaire permanent.Liste des écarts d'inventaire.Formation du personnel comptable.	<ul style="list-style-type: none">Sur- ou sous-estimation de la valeur des stocks (états financiers erronés).	<ul style="list-style-type: none">Formalisation d'une procédure de suivi des stocks et de mise à jour de l'inventaire permanent.Formalisation d'une procédure d'inventaire physique.Formation des personnes concernées en matière de valorisation et de dépréciation des stocks.
10. Certification des comptes	<ul style="list-style-type: none">Être sûr de la conformité des états financiers de l'organisation.	<ul style="list-style-type: none">Méconnaissances des règles comptables, fiscales et juridiques.	<ul style="list-style-type: none">Procédure permettant de vérifier la sincérité et la régularité des comptes annuels.	<ul style="list-style-type: none">Non-certification des comptes.Dégradation de l'image de l'entreprise.	<ul style="list-style-type: none">Mettre en place des dispositifs afin de promouvoir les bonnes pratiques professionnelles comptables.
	<ul style="list-style-type: none">Être sûr que le CAC remplit ses obligations dans le cadre de sa mission légale.	<ul style="list-style-type: none">Le CAC n'apporte pas de contribution au niveau de l'appréciation du contrôle interne.Le CAC outrepatte ses prérogatives concernant sa mission.	<ul style="list-style-type: none">Engagement de confidentialité du CAC.Collaboration entre l'audit interne et le CAC.Rapport du CAC sur le contrôle interne.	<ul style="list-style-type: none">Risque d'intrusion du CAC au-delà de ses prérogatives.Mise en péril de l'indépendance du CAC.	<ul style="list-style-type: none">Définir la mission du CAC (périmètre d'intervention, obligations et limites).Désigner une personne en interne en charge du suivi du processus de certification des comptes de l'entreprise.
11. Fiscalité	<ul style="list-style-type: none">Être sûr que l'organisation est en conformité avec la fiscalité en vigueur.	<ul style="list-style-type: none">Manque d'informations.Méconnaissance de la réglementation fiscale en vigueur.	<ul style="list-style-type: none">Entretiens.Rapprochement entre les postes relatifs aux taxes, le CA et les stocks.Mémento fiscal.	<ul style="list-style-type: none">Fraude fiscale.Opportunités fiscales non exploitées.Mauvaise image de l'entreprise.	<ul style="list-style-type: none">Mettre en place une veille sur les nouvelles réglementations en vigueur.Désigner un expert en fiscalité (interne ou externe) chargé de superviser l'application effective des règles.

PROCESSUS ET/OU DOMAINE : finance – comptabilité					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
12. Investissement	– Être sûr que les projets d'investissement sont définis, autorisés par une personne habilitée et en adéquation avec la stratégie de l'organisation.	– Procédure d'investissement absente ou mal définie ou mal connue. – Absence d'outils d'évaluation.	– Procédure d'investissement existante. – Définitions des fonctions concernées. – Mode de calcul de la rentabilité. – Dossiers d'investissement récents et significatifs (appréciation du respect de la procédure).	– Inadéquation du projet d'investissement à la stratégie de la société. – Absence de maîtrise du projet d'investissement.	– Existence, connaissance et respect d'une procédure d'investissement. – Existence et connaissance des outils pour le choix de l'investissement.
	– Être sûr que les modes de financement des investissements retenus sont judicieux.	– Procédure de financement absente, mal définie ou mal connue. – Absence d'outils d'évaluation.	– Critères de choix des modes de financement. – Dossiers d'investissement récents et significatifs (appréciation du choix du mode de financement).	– Surcoût financier.	– Existence, connaissance et respect d'une procédure de financement. – Existence et connaissance des outils pour le choix de l'investissement.

PROCESSUS ET/OU DOMAINE : juridique et fiscal					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. Juridique					
A.1. Forme juridique de l'entité	– Être sûr que la forme juridique de l'entreprise est adaptée à l'organisation.	– Statuts de la société non connus. – Statuts de l'entité incohérents avec sa finalité. – Méconnaissance des législations locales dans le cas de filiales (poids des partenaires locaux...).	– Statuts de la société. – Document Kbis. – Textes législatifs.	– Les garanties liées aux statuts ne sont pas mises en place. – Risques de sanctions fiscales. – Pertes d'opportunités fiscales (crédits d'impôts...).	– Vérifier l'existence et l'archivage des documents de constitution de l'entité. – Vérifier si toutes les dispositions et garanties prévues dans les statuts sont bien appliquées. – Désigner un expert juridique (interne ou externe) en charge de ces problématiques.
A.2. Définition et mise en œuvre des instances de gouvernance de l'organisation	– Être sûr que l'organisation est pilotée par une gouvernance d'entreprise clairement définie et conforme aux obligations légales.	– Non-respect de la législation. – Direction générale non impliquée.	– Comptes rendus de l'assemblée générale ordinaire et extraordinaire. – Comptes rendus des réunions du conseil d'administration. – Comptes rendus des réunions des divers comités, émanations du conseil (comité d'audit, des rémunérations, des risques, d'attribution des marchés...).	– Risque de fraude. – Absence de déontologie si la direction ne montre pas l'exemple. – Absence de pilotage, mettant en péril la pérennité de l'organisation. – Absence de contre- pouvoirs. – Absence de délégation.	– Mettre en œuvre des bonnes pratiques en matière de gouvernance. – Formaliser des procédures définissant les modalités de fonctionnement des divers comités, émanations du conseil (attributions, composition, fréquence des réunions, nature et délais de mise à disposition des documents préparatoires...).

PROCESSUS ET/OU DOMAINE : juridique et fiscal					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. JURIDIQUE					
A.3. Législation et réglementation	<ul style="list-style-type: none">Être sûr du respect de l'ensemble des lois et réglementations.	<ul style="list-style-type: none">Méconnaissance et non-respect des lois et réglementations (lois et réglementations locales dans le cas de filiales).Méconnaissance des activités de l'organisation par le service juridique.Pas de veille juridique.	<ul style="list-style-type: none">Textes législatifs et réglementaires.Procédure de veille juridique.	<ul style="list-style-type: none">Sanctions envers l'entreprise pour le non-respect de la législation et/ou réglementation.Atteinte à l'image et à la réputation de l'entreprise.Personnel non informé sur ses droits : risque de conflit.	<ul style="list-style-type: none">Diffuser une culture juridique dans l'organisation.Désigner un expert juridique (interne ou externe) en charge de ces problématiques.Mettre en œuvre une veille juridique (ou s'appuyer, dans le cas de filiales, sur les compétences de la maison mère en la matière).
A.4. Actifs corporels de l'entreprise	<ul style="list-style-type: none">Être sûr de la protection des actifs qui constituent le patrimoine de l'entreprise.	<ul style="list-style-type: none">Moyens de protection inefficaces ou absents.Immobilisations non couvertes par une assurance ou couvertes plusieurs fois.	<ul style="list-style-type: none">Dispositifs matériels de protection des actifs corporels.Contrats d'assurance, inventaire exhaustif des immobilisations.Système de suivi des immobilisations.	<ul style="list-style-type: none">Pertes d'actifs non assurés suite à un sinistre.Litiges avec la société d'assurance.Charges d'assurance excessives non justifiées.	<ul style="list-style-type: none">Sécuriser les actifs de l'entreprise (moyens matériels de protection adaptés).Mettre en place une couverture des risques par des contrats d'assurance adaptés (un seul contrat pour tous les biens devant être couverts).Actualiser régulièrement l'ensemble des contrats d'assurance en fonction de la situation patrimoniale de l'organisation.

PROCESSUS ET/OU DOMAINE : juridique et fiscal					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. JURIDIQUE					
A.5. Contrats	– Être sûr que les contrats sont rédigés conformément aux lois et réglementations.	– Absence de suivi des contrats. – Méconnaissance des lois et réglementations. – Non-respect du code éthique de l'organisation. – Pas de consultation entre le service juridique et les managers.	– Liste des contrats (par typologie avec dates de signature et de renouvellement). – Textes réglementaires. – Procédure de rédaction et de suivi des contrats.	– Sanctions envers l'organisation qui peuvent affecter son image et sa réputation. – Engagements mal maîtrisés, et pouvant entraîner des pertes financières. – Non-atteinte de certains objectifs.	– Formaliser une procédure de rédaction et de suivi des contrats. – Mettre en place des trames de contrats validées par la maison mère dans le cas de filiales.
	– Être sûr que les contrats sont signés par des personnes habilitées.	– Absence (ou non-mise à jour) de liste de personnes habilitées. – Méconnaissance des obligations en la matière.	– Liste des habilitations et délégations de signatures.	– Sanctions envers l'organisation qui peuvent affecter son image et sa réputation. – Engagements mal maîtrisés, et pouvant entraîner des pertes financières.	– Établir une liste limitée de personnes habilitées à signer (par catégorie de contrats).

PROCESSUS ET/OU DOMAINE : juridique et fiscal					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. Juridique					
A.6. Brevets et licences	<ul style="list-style-type: none">Être sûr du dépôt et du suivi des brevets, marques, licences et autres éléments constituant la propriété intellectuelle de l'organisation.	<ul style="list-style-type: none">Brevets non déposés ou trop tardivement.Pas de suivi des brevets.Non-renouvellement des contrats et des licences.Absence de règles de confidentialité concernant la publication et l'utilisation des brevets.Accès aux brevets non définis.	<ul style="list-style-type: none">Répertoire de l'ensemble des brevets et licences.Dispositifs de suivi périodique des brevets.Charte de confidentialité au niveau des personnes ayant accès aux brevets.Liste de personnes ayant accès aux brevets.	<ul style="list-style-type: none">Perte de propriété intellectuelle.Perte d'avantages concurrentiels.Difficultés à ordonnancer les brevets.Risque de litiges en cas de brevets, marques, licences déjà existants.	<ul style="list-style-type: none">Formaliser une procédure précisant les modalités à suivre pour le dépôt et le suivi des brevets, licences... (responsables internes concernés, instances externes à contacter, clauses...).Associer un expert juridique (interne ou externe) à la supervision de l'établissement des brevets, licences...Établir une liste des personnes habilitées à accéder aux brevets.
A.7. Litiges	<ul style="list-style-type: none">Être sûr de la maîtrise du suivi des litiges (réduction des montants de dommages et intérêts, limitation de l'impact sur l'image de l'organisation).	<ul style="list-style-type: none">Absence de directives en la matière.Pas de suivi de recouvrement des créances.Manque de compétences en matière de gestion des litiges.	<ul style="list-style-type: none">Organigramme et définitions de fonction concernées.Directives existantes en la matière.Cas de litiges récents et significatifs.Coûts des litiges en cours et passés.	<ul style="list-style-type: none">Pertes financières liées au paiement des dommages et intérêts.Provisions sur/sous-estimées, ce qui entache l'exactitude des comptes de l'entreprise.Sanctions pénales qui peuvent ternir l'image et la réputation de l'organisation.Poursuites engagées par des tiers : risque de dégradation de l'image de l'organisation.	<ul style="list-style-type: none">Associer un expert juridique au traitement des litiges.Formaliser une procédure pour le traitement des litiges (responsables internes concernés, planning, instances externes à contacter...).Mettre en œuvre une veille juridique.Formaliser une procédure pour le recouvrement des créances.Définir une méthode d'évaluation des provisions pour risques.

PROCESSUS ET/OU DOMAINE : juridique et fiscal					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. Juridique					
A.8. Droit commercial	<ul style="list-style-type: none">Être sûr de la bonne application de la réglementation liée au droit commercial.	<ul style="list-style-type: none">Incapacité des signataires.Absence de liste de personnes habilitées à signer.Méconnaissance de la réglementation en la matière et de son évolution.	<ul style="list-style-type: none">Organigramme et définitions de fonction.Liste des personnes habilitées à signer.Code de commerce et Code des marchés publics.Procédure de veille juridique existante.	<ul style="list-style-type: none">Nullité du contrat.Risques de litiges clients.Engagement de la responsabilité de l'organisation.Dégradation de l'image de l'organisation.	<ul style="list-style-type: none">Établir une liste de personnes habilitées à signer les documents engageant l'organisation.Associer un expert juridique (interne ou externe) en charge de superviser les opérations en la matière en concertation avec les responsables commerciaux.Mettre en place une veille juridique.Sensibiliser le personnel associé à l'activité commerciale à la réglementation en vigueur.Mener éventuellement des actions de formation auprès de cette population.
A.9. Droit social	<ul style="list-style-type: none">Être sûr de la bonne application de la réglementation liée au droit du travail.	<ul style="list-style-type: none">Méconnaissance de la réglementation en vigueur et de son évolution.Absence de liste de personnes habilitées à signer.	<ul style="list-style-type: none">Organigramme et définitions de fonction.Liste de personnes habilitées à signer.Contrats de travail.Conventions collectives.Charte d'éthique et règlement intérieur.Affichage des règles de sécurité.Procédure de veille juridique.	<ul style="list-style-type: none">Nullité des contrats.Dédommagements financiers.Dégradation de l'image de l'organisation.Conflits sociaux.	<ul style="list-style-type: none">Établir une liste de personnes habilitées à signer les documents engageant l'organisation.Associer un expert juridique (interne ou externe) en charge de superviser les opérations en la matière en concertation avec les responsables des ressources humaines.Mettre en place une veille juridique.Sensibiliser le personnel associé à l'activité des ressources humaines à la réglementation en vigueur.Mener éventuellement des actions de formation auprès de cette population.

PROCESSUS ET/OU DOMAINE : juridique et fiscal				
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES		EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)				
A. JURIDIQUE				
	<ul style="list-style-type: none">Être sûr que l'entreprise transmet correctement les déclarations nécessaires aux organismes sociaux.	<ul style="list-style-type: none">Absence de procédures/responsables pour les déclarations obligatoires.Tous les destinataires des déclarations sociales ne sont pas informés.Les déclarations sont incomplètes.	<ul style="list-style-type: none">Liste des destinataires : législateurs, internes à l'organisation.Échéancier de tenue des RDV sociaux prévus par la législation.PV des CE.Instructions de rédaction des déclarations.	<ul style="list-style-type: none">Nullité des contrats.Pénalités financières en cas de retards de transmission.Engagement de la responsabilité de l'employeur.Redressements en cas d'erreurs. <ul style="list-style-type: none">Formaliser une procédure précisant les modalités à suivre pour établir et transmettre les déclarations nécessaires aux organismes sociaux (responsabilités, planning, instances externes concernées, nature des informations à transmettre...).Sensibiliser/former le personnel associé à l'activité des ressources humaines à la réglementation en vigueur.Mettre en place une veille réglementaire en la matière.
B. FISCAL				
B.1. Déclarations fiscales	<ul style="list-style-type: none">Être sûr de la fiabilité des déclarations fiscales et du respect des délais dans la transmission de ces documents à l'administration fiscale concernée.	<ul style="list-style-type: none">Méconnaissance et/ou incompréhension des réglementations en vigueur.Les informations servant de base à la préparation des documents fiscaux sont incomplètes ou inexactes.	<ul style="list-style-type: none">Lois et réglementations fiscales.Liasse fiscale.Liste et planning répertoriant toutes les obligations fiscales.Pratiques régissant les modalités de réponse à ces obligations.	<ul style="list-style-type: none">Non-respect ou non-conformité avec la réglementation fiscale en vigueur : pénalités de retard, amendes...Dégradation de l'image de l'organisation. <ul style="list-style-type: none">Établir un calendrier répertoriant toutes les obligations fiscales avec les responsables concernés.Associer un expert fiscaliste (interne ou externe) chargé d'accompagner et/ou de superviser l'établissement et la transmission des déclarations fiscales.

PROCESSUS ET/OU DOMAINE : juridique et fiscal					
Étapes/ Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
B. FISCAL					
B.2. Optimisation fiscale	<ul style="list-style-type: none">Être sûr de l'optimisation fiscale et de la minimisation des impôts et taxes.	<ul style="list-style-type: none">Les informations permettant de générer des économies d'impôts ne sont pas connues.Absence de veille fiscale.	<ul style="list-style-type: none">Déclarations faites à l'administration fiscale (TP, TS, CS, etc.).Benchmarking : comparer le montant des charges fiscales d'entreprises de nature et de taille comparable.Code général des impôts.Procédure de veille fiscale existante.	<ul style="list-style-type: none">Opportunités d'économies d'impôt non saisies.Paiement d'impôts et de taxes injustifiés.	<ul style="list-style-type: none">Examiner les déclarations et la situation fiscale périodiquement afin d'identifier des possibilités d'optimisation fiscale.S'assurer que le personnel concerné est informé de la réglementation fiscale et de son évolution.Mener une réflexion sur l'adaptation du régime fiscal de l'organisation par rapport à ses performances, son secteur d'activité, sa situation géographique...
B.3. Paiement des impôts et taxes	<ul style="list-style-type: none">Être sûr du respect des échéances de règlement.	<ul style="list-style-type: none">Méconnaissance des obligations en la matière.	<ul style="list-style-type: none">Pratiques existantes (échéancier de règlement...).Code général des impôts.	<ul style="list-style-type: none">Pénalités financières pour retard de paiement.Dégradation de l'image de l'organisation.Risque de poursuites et de non-certification des comptes.	<ul style="list-style-type: none">Établir un échéancier « fiscal ».Veiller à sa bonne application.Sensibiliser le personnel en charge du paiement des impôts et taxes au respect des échéances de règlement.

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. MESURE DE LA PERFORMANCE					
A.1. Choix des indicateurs de mesure de la performance	<ul style="list-style-type: none">Être sûr de la pertinence du choix des indicateurs de mesure de la performance réelle de l'organisation.	<ul style="list-style-type: none">Sélection unilatérale des indicateurs de mesure par le contrôle de gestion sans réelle concertation avec les responsables des activités concernées et la gouvernance de l'organisation.	<ul style="list-style-type: none">Tableaux de bord existants (reporting).Comptes rendus de réunion entre le contrôle de gestion et les utilisateurs de ces indicateurs, attestant d'une réelle concertation lors du choix des indicateurs de mesure de la performance.Notes sur les éventuelles remises en question du choix initial.	<ul style="list-style-type: none">Indicateurs retenus non pertinents par rapport aux problématiques de mesure de la performance de l'organisation.Désintérêt des responsables concernés pour cette démarche.	<ul style="list-style-type: none">Établir les critères de choix des indicateurs de mesure de la performance en concertation avec les responsables concernés.Tenir compte des capacités du système d'information à fournir les informations nécessaires.
A.2. Informations nécessaires à la valorisation des indicateurs	<ul style="list-style-type: none">Être sûr que les informations nécessaires à la valorisation des indicateurs sont disponibles et fiables.	<ul style="list-style-type: none">Système d'information ne fournissant pas les informations nécessaires.	<ul style="list-style-type: none">Système d'information utilisé.Difficultés rencontrées au niveau de la récolte des informations nécessaires.	<ul style="list-style-type: none">Non-fiabilité des indicateurs fournis.Retard dans la communication des tableaux de bord.	<ul style="list-style-type: none">Formaliser une procédure définissant les modalités de calcul des indicateurs de mesure de la performance (outils informatiques utilisés, informations nécessaires, étapes de calcul, périodicité, forme, exploitation des résultats...).

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. MESURE DE LA PERFORMANCE					
A.3. Définition des tableaux de bord	<ul style="list-style-type: none">Être sûr que les tableaux de bord destinés à chaque responsable sont pertinents (nature et nombre d'indicateurs, périodicité, forme...) au regard des prises de décisions qu'ils doivent permettre d'éclairer.	<ul style="list-style-type: none">Non-consultation des responsables concernés par l'utilisation des indicateurs.Décision unilatérale du contrôle de gestion.	<ul style="list-style-type: none">Tableaux de bord existants.Entretien avec le contrôle de gestion et les responsables concernés afin d'apprécier si les tableaux de bord répondent aux besoins des utilisateurs.	<ul style="list-style-type: none">Tableaux de bord inadaptés au pilotage des activités.Performance de l'entreprise compromise car outil d'aide à la décision inexploitable.	<ul style="list-style-type: none">Formaliser une procédure définissant les modalités de calcul des indicateurs de mesure de la performance (outils informatiques utilisés, informations nécessaires, étapes de calcul, périodicité, forme, exploitation des résultats...).Associer les utilisateurs des indicateurs de mesure de la performance à la conception des tableaux de bord.
A.4. Conseils apportés aux responsables concernés dans le pilotage de leur activité	<ul style="list-style-type: none">Être sûr de l'utilisation pertinente des indicateurs de mesure de la performance.	<ul style="list-style-type: none">Exploitation informelle et/ou non systématique des indicateurs.Non-communication de ces résultats aux responsables concernés.Absence de concertation entre le contrôle de gestion et les responsables concernés.	<ul style="list-style-type: none">Procédure d'élaboration des tableaux de bord (si elle existe).Comptes rendus de réunions entre le service contrôle de gestion et les responsables concernés pour expliquer les évolutions constatées et les causes possibles.	<ul style="list-style-type: none">Désintérêt des responsables concernés concernant l'utilisation des tableaux de bord dans le pilotage de leur activité.Gaspillage de ressources.Absence d'outils de pilotage et de prises de décision.	<ul style="list-style-type: none">Formaliser une procédure définissant les modalités de calcul des indicateurs de mesure de la performance (outils informatiques utilisés, informations nécessaires, étapes de calcul, périodicité, forme, exploitation des résultats...).Réaliser des réunions périodiques entre le service de contrôle interne et les destinataires des tableaux de bord.

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
A. MESURE DE LA PERFORMANCE					
A.5. Communication des résultats à la direction générale et/ou aux instances de gouvernance	<ul style="list-style-type: none">Être sûr qu'une synthèse périodique de ces indicateurs de mesure de la performance est faite à la direction générale et/ou aux instances de gouvernance.	<ul style="list-style-type: none">Manque d'intérêt de la direction générale (et/ou instances de gouvernance) concernant la mesure de la performance.Synthèse des indicateurs de mesure de la performance inadaptée aux attentes de la direction générale.Absence de communication des tableaux à la direction générale et/ou aux instances de gouvernance.	<ul style="list-style-type: none">Organigramme et définitions de fonctions.Liste des personnes destinataires des tableaux de bord.Comptes rendus de réunion avec la direction générale concernant l'analyse de la synthèse des indicateurs de mesure de la performance.	<ul style="list-style-type: none">Mauvaise interprétation de l'information, entraînant une mauvaise orientation dans la prise de décision/le choix stratégique.Manque de réactivité dans la prise de décision.	<ul style="list-style-type: none">Formaliser une procédure définissant les modalités de calcul des indicateurs de mesure de la performance (outils informatiques utilisés, informations nécessaires, étapes de calcul, périodicité, forme, exploitation des résultats...).Définir la nature et la forme des synthèses à faire auprès de la direction générale (et/ou les instances de gouvernance) sur les indicateurs de mesure de la performance.

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
B. DÉMARCHE BUDGÉTAIRE					
B.1. Construction des budgets	<ul style="list-style-type: none">Être sûr que les budgets sont élaborés de façon pertinente et en cohérence avec les objectifs de l'organisation.	<ul style="list-style-type: none">Absence ou imprécision des objectifs généraux de l'organisation et de leurs déclinaisons en objectifs opérationnels.Concertation insuffisante entre l'équipe en charge de la construction des budgets (service contrôle de gestion) et les responsables de centres budgétaires.Orientations budgétaires fixées unilatéralement par la direction générale sans implication des responsables de centre budgétaire.Informations insuffisantes et/ou non fiables nécessaires à la construction des budgets.	<ul style="list-style-type: none">Procédure budgétaire (si elle existe).Liste des objectifs généraux de l'organisation et leurs déclinaisons en objectifs opérationnels.Planning précisant les étapes budgétaires (construction, suivi et contrôle...).Résultats du contrôle budgétaire de l'exercice précédent (appréciation de la fiabilité des prévisions budgétaires).	<ul style="list-style-type: none">Budgets en décalage avec les objectifs généraux et la stratégie de l'organisation.Découpage budgétaire sans cohérence avec la répartition des responsabilités dans l'organisation.Non-fiabilité des prévisions budgétaires.Désintérêt des responsables de centre budgétaire pour la démarche.	<ul style="list-style-type: none">Établir un planning des étapes jalonnant la démarche budgétaire.Formaliser une procédure pour la démarche budgétaire (responsabilités, informations initiales nécessaires, interlocuteurs concernés, modalités de suivi et de contrôle, exploitation des résultats...).Définir les modalités de révision des budgets (événements justifiant cette révision, périodicité de la révision...).Faire participer les responsables des centres budgétaires à l'élaboration des budgets.

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
B. DÉMARCHE BUDGÉTAIRE					
B.2. Suivi et contrôle budgétaire	<ul style="list-style-type: none">Être sûr que les budgets font l'objet d'un suivi et d'un contrôle périodique tout au long de la période budgétaire.	<ul style="list-style-type: none">Absence de suivi et de contrôle budgétaire.Suivi et contrôle budgétaire non réguliers et/ou informels.	<ul style="list-style-type: none">Procédure budgétaire (si elle existe).Résultats du contrôle budgétaire de l'exercice précédent (appréciation de la réalité de ces contrôles).Planning précisant les étapes budgétaires (construction, suivi et contrôle...).	<ul style="list-style-type: none">Désintérêt des responsables de centre budgétaire pour la démarche.Gaspillage de ressources.	<ul style="list-style-type: none">Formaliser une procédure pour la démarche budgétaire (responsabilités, informations initiales nécessaires, interlocuteurs concernés, modalités de suivi et de contrôle, exploitation des résultats...).
B.3. Exploitation des résultats du contrôle budgétaire	<ul style="list-style-type: none">Être sûr de l'utilisation pertinente des résultats du contrôle budgétaire tout au long de la période.	<ul style="list-style-type: none">Exploitation informelle des résultats du contrôle budgétaire.Non-communication de ces résultats aux responsables de centre budgétaire.	<ul style="list-style-type: none">Procédure budgétaire (si elle existe).Comptes rendus de réunions entre le service contrôle de gestion et les responsables de centre budgétaire pour expliquer les écarts budgétaires éventuels.	<ul style="list-style-type: none">Désintérêt des responsables de centre budgétaire pour la démarche.Gaspillage de ressources.	<ul style="list-style-type: none">Formaliser une procédure pour la démarche budgétaire (responsabilités, informations initiales nécessaires, interlocuteurs concernés, modalités de suivi et de contrôle, exploitation des résultats...).Réaliser des réunions périodiques tout au long de l'exercice.
B.4. Supports de la démarche budgétaire	<ul style="list-style-type: none">Être sûr que la démarche budgétaire est supportée par des outils adaptés et performants (système d'information, méthode structurée...).	<ul style="list-style-type: none">Absence ou insuffisance des supports informatiques pour la démarche.Responsabilités mal définies.Absence de méthode.	<ul style="list-style-type: none">Outils informatiques existants.Liste des personnes responsables concernées.	<ul style="list-style-type: none">Lentement dans le traitement des opérations.	<ul style="list-style-type: none">Établir une liste des personnes concernées par la démarche budgétaire.Disposer d'applicatifs informatiques encadrant la démarche.

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
C. CALCUL DES COÛTS					
C.1. Choix des thématiques nécessitant un calcul des coûts (produits/services, commandes spécifiques...)	<ul style="list-style-type: none">Être sûr que les moyens mis en œuvre pour le calcul des coûts (humains, technologiques...) sont affectés, de façon pertinente, aux réelles problématiques de connaissance des coûts.	<ul style="list-style-type: none">Absence de réflexion concernant l'affectation des moyens disponibles en la matière.Manque de moyens (effectif du service contrôle de gestion, compétences...).	<ul style="list-style-type: none">Entretiens avec les responsables du service contrôle de gestion.Justification des choix retenus en matière d'affectation des moyens.	<ul style="list-style-type: none">Mauvaise affectation des moyens.Absence d'information concernant les réelles problématiques de connaissance des coûts en fonction des enjeux de l'organisation.	<ul style="list-style-type: none">Définir les responsabilités en matière de choix des thématiques de calcul des coûts (communication entre le service contrôle interne et les responsables des coûts calculés).
C.2. Choix et application des méthodes de calcul des coûts	<ul style="list-style-type: none">Être sûr que le choix des méthodes de calcul des coûts est judicieux en fonction de la finalité recherchée.	<ul style="list-style-type: none">Méconnaissance des principes et méthodes de calcul des coûts.Méconnaissance des obligations réglementaires en la matière (valorisation « fiscale » des stocks).	<ul style="list-style-type: none">Méthodes de calcul de coûts pratiquées.Justification des choix retenus en matière de choix des méthodes.	<ul style="list-style-type: none">Précision et/ou fiabilité des coûts calculés inadaptées aux besoins de l'organisation.	<ul style="list-style-type: none">Définir les critères permettant le choix des méthodes de calcul des coûts.Former les contrôleurs de gestion aux méthodes de calcul des coûts.Formaliser une procédure définissant les modalités de calcul des coûts pour la ou les méthodes pratiquées (outils informatiques utilisés, informations nécessaires, étapes de calcul, exploitation des résultats...).
	<ul style="list-style-type: none">Être sûr que les méthodes de calcul retenues sont correctement mises en œuvre.	<ul style="list-style-type: none">Méconnaissance des principes et méthodes de calcul des coûts.Système d'information inadapté à la mise en œuvre des méthodes de calcul.	<ul style="list-style-type: none">Appréciation des pratiques lors de l'application des méthodes de calcul des coûts.Système d'information utilisé.	<ul style="list-style-type: none">Non-fiabilité des coûts calculés.	

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
C. CALCUL DES COÛTS					
C.3. Informations nécessaires au calcul des coûts	– Être sûr que les informations nécessaires au calcul des coûts sont disponibles et fiables.	– Système d'information ne fournissant pas les informations nécessaires.	– Système d'information utilisé. – Difficultés rencontrées au niveau de la récolte des informations nécessaires.	– Non-fiabilité des coûts calculés.	– Formaliser une procédure définissant les modalités de calcul des coûts pour la ou les méthodes pratiques (outils informatiques utilisés, informations nécessaires, étapes de calcul, exploitation des résultats...).
C.4. Exploitation des résultats de ces calculs de coûts	– Être sûr que les résultats des calculs de coûts sont exploités de façon pertinente, afin de répondre aux besoins des demandeurs.	– Absence ou insuffisance de communication entre le service contrôle de gestion et les utilisateurs concernés par les coûts calculés.	– Comptes rendus de réunion entre le service contrôle de gestion et les responsables concernés par les coûts calculés. – Organigramme et définitions de fonction.	– Insatisfaction des demandeurs concernés par les coûts calculés. – Prises de décisions incertaines en l'absence d'éclairage précis sur les coûts.	– Formaliser une procédure définissant les modalités de calcul des coûts pour la ou les méthodes pratiques (outils informatiques utilisés, informations nécessaires, étapes de calcul, exploitations des résultats...).
D. REPORTING À LA MAISON MÈRE (CAS D'UNE FILIALE)					
D.1. Connaissance des exigences de reporting à la maison mère	– Être sûr que la filiale adhère à la politique de reporting du groupe.	– Absence ou mauvaise communication de la part de la maison mère concernant la nécessité et l'importance d'un reporting au niveau du groupe. – Intérêt relatif de la filiale qui n'en comprend pas l'utilité et qui vit ces obligations comme une contrainte.	– Procédure de reporting (si elle existe). – Tableaux de reporting récents. – Documents communiqués par la maison mère pour sensibiliser la filiale à ce dispositif. – Entretiens avec les responsables en filiale et à la maison mère en charge de ces opérations.	– Désintérêt de la filiale pour le reporting.	– Communiquer au niveau du groupe sur la nécessité et l'importance d'un reporting fiable à des fins de consolidation. – Formaliser une procédure reporting au niveau du groupe (responsables concernés, planning de transmission de l'information, explication de la nature des informations demandées...).

PROCESSUS ET/OU DOMAINE : contrôle de gestion – reporting					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE					
(découpage du processus et/ou domaine de gestion)					
D. REPORTING À LA MAISON MÈRE (CAS D'UNE FILIALE)					
D.2. Informations nécessaires à l'alimentation du reporting	<ul style="list-style-type: none">Être sûr de la fiabilité du reporting à des fins de consolidation au niveau du groupe.	<ul style="list-style-type: none">Décalage entre la nature des informations demandées dans le reporting et celles disponibles au niveau du système d'information de la filiale.Informations alimentant le reporting non fiables.	<ul style="list-style-type: none">Procédure de reporting (si elle existe).Tableaux de reporting récents.Entretiens avec les responsables en filiale et à la maison mère en charge de ces opérations.Modalités d'exploitation du reporting à la maison mère.	<ul style="list-style-type: none">Non-fiabilité de la consolidation au niveau du groupe, d'où des prises de décisions stratégiques non fondées.	<ul style="list-style-type: none">S'assurer, lors de la conception des tableaux de reporting, de la capacité de toutes les filiales consolidées à les alimenter de façon fiable et dans les délais prévus.Formaliser une procédure de reporting au niveau du groupe (responsables concernés, planning de transmission de l'information, explication de la nature des informations demandées...).
D.3. Communication du reporting à la maison mère	<ul style="list-style-type: none">Être sûr du respect des exigences de reporting par la filiale (délais...).	<ul style="list-style-type: none">Intérêt relatif de la filiale qui n'en comprend pas l'utilité et qui vit ces obligations comme une contrainte.Sources d'informations alimentant le reporting non disponibles.	<ul style="list-style-type: none">Entretiens avec les responsables en filiale et à la maison mère en charge de ces opérations.Dates réelles de transmission des tableaux de reporting comparées au planning prévu.	<ul style="list-style-type: none">Retard dans la transmission du reporting et donc dans la consolidation du groupe.	<ul style="list-style-type: none">Formaliser une procédure de reporting au niveau du groupe (responsables concernés, planning de transmission de l'information, explication de la nature des informations demandées...).

PROCESSUS ET/OU DOMAINE : systèmes d'information					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
1. Accès aux systèmes d'information	<ul style="list-style-type: none">Être sûr que seules les personnes autorisées ont accès aux systèmes d'information.	<ul style="list-style-type: none">Accès au système d'information non contrôlé.Non-mise à jour des listes de personnes autorisées (notamment lors de départ de salariés).Absence de confidentialité au niveau de la connaissance des codes d'accès.	<ul style="list-style-type: none">Liste de personnes habilitées ayant accès au SI.Liste des <i>logins</i> et mots de passe.Procédure de mise à jour des <i>logins</i> et mots de passe.Procédure de départ des salariés.Historique des connexions.Hierarchisation des informations présentes sur le SI en fonction du degré de confidentialité.	<ul style="list-style-type: none">Perte de confidentialité.Perte de qualité/intégrité des informations.Absence de détection de modification de fichiers/données sensibles.Risques de fraude.Risque financier.Fuite de données stratégiques à la concurrence.	<ul style="list-style-type: none">Établir la liste des autorisations d'accès au SI, aux applications et aux fichiers/données sensibles : codes d'accès, outils de gestion des accès (tables d'accès par identifiant, notion de groupe d'utilisateurs, différenciation lecture/écriture...).Formaliser une procédure d'attribution (arrivée, mutation), de suppression et de mise à jour des mots de passe et codes d'accès.Désigner un responsable de l'attribution des niveaux de confidentialité et de la gestion des autorisations d'accès.Revoir périodiquement la liste des <i>logins</i> et mots de passe actifs.Définir le principe de séparation de fonctions dans la gestion des autorisations d'accès (séparation décision/réalisation).
2. Sécurité physique des systèmes informatiques	<ul style="list-style-type: none">Être sûr qu'il existe un système de sécurité adapté permettant de protéger les données informatiques contre les pirates, les virus, les pannes électriques, la foudre...	<ul style="list-style-type: none">Destruction ou altération du matériel et/ou des fichiers.Obsolescence des équipements (<i>hardware</i> et <i>software</i>).Non-sécurisation externe du SI.Dispositif de sécurité incendie insuffisant.	<ul style="list-style-type: none">Liste des différents dispositifs de sécurité.Modalités de fonctionnement des dispositifs de sécurité.Procédure de mise à jour périodique des outils de sécurité.	<ul style="list-style-type: none">Reprise compromise de l'exploitation.Perte d'informations stratégiques.Diminution de la compétitivité de la société.	<ul style="list-style-type: none">Gestion des accès à la salle informatique par badge.Existence de moyens de protection des installations, matériels sensibles (calculateur central, câbles de transmission...) et supports magnétiques : protection contre l'incendie, le dégât des eaux...

PROCESSUS ET/OU DOMAINE : systèmes d'information					
Étapes/Sous-domaines	FINALITÉS (objec-tifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'em-pêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
3. Gestion des relations avec l'extérieur	– Être sûr que les relations avec les sociétés extérieures sont maîtrisées (fournisseurs, sous-traitants).	– Altération du matériel et/ou des fichiers par des tiers. – Absence de maîtrise du SI.	– Veille sur les nouvelles technologies informatiques.	– Risque financier. – Risque de fraude. – Dépendance vis-à-vis du sous-traitant. – Absence de maîtrise des projets sous-traités.	– Respect du droit d'utilisation prévu en contrat par le fournisseur du logiciel. – Existence d'une protection contre les virus.
		– Absence de maîtrise des projets sous-traités (adéquation aux besoins, respect des délais et des coûts, maintenance et évolution des applications...). – Absence de contrats de maintenance avec les prestataires de services. – Clauses de contrats inadaptées avec les prestataires de services (risque juridique). – Délai de paiement des prestataires de services non respecté (risque financier). – Absence de procédure de gestion des contrats de prestation. – Collusion avec les prestataires. – Habilitations des personnes extérieures non mises à jour. – Prestataire unique toute application : prestation de maintenance dite à 100 %.	– Modalités concernant la réception des services demandés conformément aux termes du contrat signé avec le prestataire (exhaustivité des prestations, délais...), – Liste des personnes habilitées à rédiger et signer des contrats. – Clauses contractuelles : délai, paiement... – Existence d'une procédure. – Liste des habilitations et de typologie des droits.	– Perte de confidentialité. – Risque de fuite d'informations confidentielles.	– Existence d'orientations claires concernant l'appel à la sous-traitance. – Détermination des applications sur lesquelles peuvent intervenir les prestataires et le type de travaux pouvant être sous-traités suivant le caractère stratégique de chaque application. – Existence de contrats entre la société et les prestataires de services, validés et contrôlés par un organisme compétent. – Analyse du niveau de dépendance vis-à-vis des sous-traitants. – Définition des champs d'application et des types de travaux sur lesquels les prestataires peuvent intervenir. – Existence de clauses de confidentialité adaptées. – Choix de prestataires de services certifiés. – Réception de tous les services demandés conformément aux termes du contrat. – Rédaction et signature du contrat par des personnes habilitées. – Respect des clauses du contrat : délai, paiement. – Utilisation de types de régie.

PROCESSUS ET/OU DOMAINE : systèmes d'information					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
4. Gestion des sauvegardes	<ul style="list-style-type: none">Être sûr que les données sont sauvegardées de manière périodique sur différents supports à différents endroits.	<ul style="list-style-type: none">Absence de sauvegarde systématique.Absence de hiérarchisation des données à sauvegarder.Absence de sauvegarde régulière en fonction du niveau d'importance des données.Absence de protocole de stockage de sauvegarde.Sauvegarde sur un support unique.	<ul style="list-style-type: none">Liste des sauvegardes effectuées.Correspondance du nombre des sauvegardes listées avec le niveau des stocks de sauvegardes.Codes classifiant l'importance des données.	<ul style="list-style-type: none">Risque financier.Perte d'informations stratégiques.Reprise compromise des exploitations.Incapacité à restaurer en priorité les données les plus critiques.Perte de confidentialité liée à des accès aux sauvegardes non contrôlés.	<ul style="list-style-type: none">Mise en place d'une procédure périodique de sauvegarde automatisée des données.Hiérarchisation des données à sauvegarder.Salle de confinement des sauvegardes avec des accès sécurisés et limités.Suivi par registre des personnes accédant aux sauvegardes.Procédure de restauration des données formalisée et testée de façon périodique.Compte rendu de la bonne exécution des sauvegardes.
5. Maintenance	<ul style="list-style-type: none">Être sûr de la pérennité du fonctionnement des systèmes informatiques.	<ul style="list-style-type: none">Bugs à répétition.Pas de mise à jour des programmes.Non-renouvellement des licences.Prestation de maintenance « générique » non définie.Coupure d'électricité.Sinistre ou catastrophe naturelle.	<ul style="list-style-type: none">Périodicité des contrats de maintenance.Réactivité des personnes chargées de régler les bugs : tableaux de bord des performances du service.Définition du champ d'application de la maintenance.Classification des bugs génériques.	<ul style="list-style-type: none">Problèmes d'accès au SI.Perte éventuelle des données.Non-utilisation du SI car vu comme étant « contraignant et lourd ».Utilisation de SI parallèles (PC personnels etc.).Interruption de l'activité.	<ul style="list-style-type: none">Existence de moyens pour reprendre l'exploitation en cas de panne ou de perte importante de données (plan de reprise, contrat de maintenance...).Existence d'une hotline/personnes dédiées (interne ou externe).Reporting des bugs rencontrés (machine, circonstance, explications).Création d'un service de maintenance interne : hotline, service client...Existence d'un local externe pour assurer la sauvegarde des données en cas de sinistre/catastrophe naturelle.Mise en place d'onduleurs, groupes électrogènes, etc., pour la continuité de l'alimentation des SI.

PROCESSUS ET/OU DOMAINE : systèmes d'information					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
6. Pertinence du système d'information	<ul style="list-style-type: none">Être sûr de la pertinence du système informatique au sein de la société et de son efficacité usuelle.	<ul style="list-style-type: none">Manque de personnels compétents en système d'information.Manque de matériel performant, optimisant l'utilisation des systèmes d'information.Absence de formations facilitant l'utilisation des systèmes d'information.Complexité accrue du système d'information.	<ul style="list-style-type: none">Actions périodiques de formation aux systèmes d'information.Renouvellement du matériel informatique.Cohérence entre le besoin des utilisateurs et les outils informatiques.Planning des projets informatiques.Redéfinition des applications périodiques en collaboration avec les utilisateurs.	<ul style="list-style-type: none">Inadéquation des systèmes d'information aux besoins de la société.Perte de temps.Perte d'efficacité.Non-optimisation des ressources.Insatisfaction des utilisateurs.Absence de maîtrise du volume de travaux des systèmes d'information.Risque financier (absence de maîtrise des coûts).	<ul style="list-style-type: none">Définition d'une politique de choix des matériels informatiques.Existence d'un budget et d'un suivi des coûts.Existence et pertinence des critères de choix et de hiérarchisation des développements à réaliser.Modalités d'échanges entre informatiques et utilisateurs (existence de correspondants informatiques, modalités des transmissions des demandes ou des dysfonctionnements à l'informatique).Définition d'un plan d'actions permettant l'évolution des systèmes d'information.
7. Fiabilité du système d'information	<ul style="list-style-type: none">Être sûr de la fiabilité du système d'information.	<ul style="list-style-type: none">Programme non correct ou non mis à jour.Infrastructures inadaptées pour les serveurs.Absence de possibilité de back-up.	<ul style="list-style-type: none">Procédures de développement et de maintenance (licences, contrats de maintenance).Existence d'un modèle conceptuel de données (MCD).Salles aux normes (« salles blanches »).	<ul style="list-style-type: none">Perte de qualité et d'intégrité de l'information.Dégradation accélérée du matériel.	<ul style="list-style-type: none">Existence d'un schéma décrivant l'architecture des systèmes d'information.Existence d'interfaces appropriées entre les systèmes et les applications : absence de double saisie, contrôle automatique des saisies, contrôle des échanges de données.Installation des serveurs centraux dans des locaux adaptés.

PROCESSUS ET/OU DOMAINE : systèmes d'information					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
8. Documentation	<ul style="list-style-type: none">Être sûr qu'il existe une base de documentation du système d'information disponible et mise à jour afin d'atteindre les objectifs assignés.	<ul style="list-style-type: none">Documents non mis à jour.Documentation trop complexe.Documentation absente ou incomplète.	<ul style="list-style-type: none">Procédure de gestion documentaire.Base de données documentaires.	<ul style="list-style-type: none">Machines et outils en panne impossibles à réparer dans l'immédiat.Difficultés de maintenance appropriée.Difficultés de formation des nouveaux employés.Non-utilisation des SI de manière optimale.	<ul style="list-style-type: none">Mise en place d'une documentation fournie, variée et mise à jour régulièrement.Mise à disposition de l'ensemble des documents nécessaires en temps opportuns.Dissocier documentation technique et documentation utilisateur.Créer un archivage papier en parallèle de l'archivage numérique.
9. Utilisation du système d'information	<ul style="list-style-type: none">S'assurer que les règles d'utilisation des SI sont définies et connues de tous.S'assurer que les règles d'utilisation des SI s'appliquent aux sous-traitants et autres prestataires de service.	<ul style="list-style-type: none">Absence de procédures liées à la sécurité des SI.Mauvaise diffusion des procédures.Absence de clauses de confidentialité avec les prestataires ayant accès au SI.	<ul style="list-style-type: none">Charte informatique.Diffusion/affichage de la charte informatique.Formation des collaborateurs.	<ul style="list-style-type: none">Risque lié à la sécurité des SI.Risque de fuite d'informations confidentielles.	<ul style="list-style-type: none">Rédaction d'une charte informatique.Incorporation de la charte au contrat de travail.Rédaction d'avenants aux contrats existants afin d'y ajouter la charte informatique.

PROCESSUS ET/OU DOMAINE : recherche et développement					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion de gestion)					
1. Lancement d'un projet	<ul style="list-style-type: none">Être sûr que le lancement d'un projet est conforme avec les objectifs de l'organisation, qu'il est faisable et planifié.	<ul style="list-style-type: none">Absence d'étude de coûts et/ou de faisabilité.Absence de comité de décision.Absence de planification des tâches et ressources nécessaires au projet.	<ul style="list-style-type: none">Existence et pertinence des études de coût et de faisabilité.Existence et composition du comité de décision.Existence, communication et réalisme de l'avant-projet (responsable, équipe, ressources, tâches, délai...).	<ul style="list-style-type: none">Projet incohérent avec les objectifs de l'organisation.Projet trop long, coûteux, non rentable, non faisable.Décision irrationnelle.Non-atteinte des objectifs.Pertes financières.Démotivation du personnel concerné.	<ul style="list-style-type: none">Mettre en place un comité de décision indépendant pour le lancement d'un projet R&D, réuni périodiquement.Diffuser l'information aux personnes concernées.Exiger un avant-projet systématique pour les projets évalués, comprenant des études de coûts et de faisabilité, une planification détaillée et les responsabilités.
2. Gestion des flux entre équipes	<ul style="list-style-type: none">Être sûr que les différentes équipes de R&D communiquent entre elles et capitalisent leurs savoirs.	<ul style="list-style-type: none">Équipes éloignées, ne disposant pas de système de communication et/ou de diffusion de l'information.Rétention d'information.Différences culturelles dans la façon de travailler.	<ul style="list-style-type: none">Existence et utilisation des supports de communication et de diffusion de l'information et/ou fréquence et contenu des réunions.Mise à jour des informations diffusées.Sécurité des informations partagées.	<ul style="list-style-type: none">Perte de savoir-faire.Doubletons dans les recherches.Pertes de temps.Espionnage industriel.Objectifs compromis.	<ul style="list-style-type: none">Mettre en place un système de diffusion de l'information adapté, sécurisé, documenté.Promouvoir les échanges entre équipes travaillant sur des projets différents (réunions, projets transverses...).Mettre à jour un système de partage de savoir.S'assurer de la confidentialité des informations pour éviter les fuites.Mettre en place des réunions d'état d'avancement qui mettent en avant les objectifs, l'évolution, etc.

PROCESSUS ET/OU DOMAINE : recherche et développement					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion de gestion)					
3. Travail en laboratoire, conception de prototypes	<ul style="list-style-type: none">Être sûr du suivi du travail de recherche en laboratoire.	<ul style="list-style-type: none">Absence de contrôle.Absence de planification détaillée et/ou de responsable désigné dans l'avant-projet.	<ul style="list-style-type: none">Existence et contenu des réunions de travail : conformité avec la planification de l'avant-projet.	<ul style="list-style-type: none">Allongement du projet de recherche.Perte de savoir.	<ul style="list-style-type: none">Mettre en place un dispositif de suivi de chaque projet, conforme au projet initial (possibilité de flexibilité si justification).Diviser le projet en plusieurs « étapes » pour en suivre l'avancement plus facilement.
4. Tests et expérimentations	<ul style="list-style-type: none">Être sûr que les tests et expérimentations sont menés dans les temps par les personnes habilitées, et suivis par le responsable.	<ul style="list-style-type: none">Absence de planification détaillée et/ou de responsable désigné dans l'avant-projet.	<ul style="list-style-type: none">Suivi des tests et expérimentations : rapports, réunions de travail et bilan justifié et détaillé des tests.	<ul style="list-style-type: none">Projet retardé.Tests faussés.Pertes financières.	<ul style="list-style-type: none">Mettre en place un dispositif de suivi de la phase de test et d'expérimentation avec des réunions de présentation de l'avancée des travaux et des conclusions, des rapports justifiant les conclusions.
5. Accord final de la direction	<ul style="list-style-type: none">Être sûr que la direction dispose de toutes les informations nécessaires pour prendre les décisions appropriées concernant la commercialisation du produit.	<ul style="list-style-type: none">Prise de décision sans tenir compte des informations du service R&D et de la réglementation.Prise de décision de la direction sans tenir compte des contraintes opérationnelles.	<ul style="list-style-type: none">Procédure de validation de la DG (respect des réglementations en vigueur).	<ul style="list-style-type: none">Défiance des actionnaires.Mauvais positionnement pour la maîtrise des résultats de la société.Non-atteinte des objectifs.Atteinte à l'image de l'entreprise.Pertes financières.	<ul style="list-style-type: none">Existence d'une procédure lors de l'émission d'un avis (assurant le respect des réglementations et des lois en vigueur).Existence d'une plateforme collaborative afin de centraliser les informations utiles à la prise de décision.

PROCESSUS ET/OU DOMAINE : recherche et développement					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion de gestion)					
6. Dépôt de brevet	– Être sûr de la protection juridique des produits conçus.	– Non-paiement des taxes nécessaires à l'obtention d'un brevet. – Développement d'un produit faisant déjà l'objet d'un brevet. – Dépôt tardif ou non-dépôt des brevets. – Absence de veille juridique concernant les législations sur la propriété industrielle et intellectuelle. – Non-prise en compte de la dimension géographique lors du dépôt de brevet.	– Dossier de demande d'obtention d'un brevet. – Factures établies par l'organisme d'enregistrement. – Brevets. – Certificats de l'INPI.	– Imitation et contrefaçon. – Perte d'avantage concurrentiel. – Perte financière. – Projet non rentable. – Contentieux avec d'autres dépositaires.	– Existence d'une veille concurrentielle et juridique. – Existence d'une collaboration avec le service juridique. – Mettre en place un archivage fiable des brevets.
	– Être sûr de la bonne formalisation et de la mise à jour des procédures de brevetage.	– Absence de dispositif et/ou de politique concernant les DPI. – Non-suivi des procédures/politiques de dépôt de brevet.	– Existence et pertinence du dispositif de DPI : responsable, conditions de dépôt du brevet (comité...), enregistrement. – Politique de dépôt de brevet en corrélation avec la politique de développement.	– Retard au niveau des dépôts de brevets. – Dépôts de brevets non conformes. – Perte financière.	– Élaboration d'un cahier des charges. – Mettre en place un dispositif clair concernant les DPI : comité de décision (évaluation de la rentabilité et de la pertinence de la démarche), personnes responsables, suivi des brevets.
	– Être sûr du maintien des brevets dans le temps.	– Dépassement du délai imparti quant à l'enregistrement du brevet et à sa publication.	– Existence et pertinence du dispositif de DPI : responsable, conditions de dépôt du brevet, (comité...), enregistrement.	– Perte d'avantage concurrentiel. – Perte financière. – Projet non rentable.	– Existence d'une veille concurrentielle et juridique. – Mettre en place une procédure de publication des brevets.

PROCESSUS ET/OU DOMAINE : recherche et développement					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion de gestion)					
7. Gestion du portefeuille projet	<ul style="list-style-type: none">Être sûr de la gestion des projets en cours.	<ul style="list-style-type: none">Absence de procédure de gestion des projets.	<ul style="list-style-type: none">Dispositif de suivi des projets (remontée de l'information, suivi des projets : réunions...).	<ul style="list-style-type: none">Projets non menés à terme.Non-atteinte des objectifs organisationnels.	<ul style="list-style-type: none">S'assurer périodiquement que tous les projets s'inscrivent dans la ligne définie par la R&D et en cohérence avec les objectifs stratégiques de l'organisation.
8. Conception des procédés de production	<ul style="list-style-type: none">Être sûr que les innovations se traduisent par l'industrialisation des produits concernés.	<ul style="list-style-type: none">Objectifs de la R&D peu clairs.Mauvaise communication avec la production.	<ul style="list-style-type: none">Évaluation et suivi de la conception des procédés de production à grande échelle (lien avec le bureau d'étude).	<ul style="list-style-type: none">Doublons, superposition des tâches avec le bureau d'étude.Innovation non appliquée.	<ul style="list-style-type: none">Mettre en place un lien privilégié entre la R&D et le bureau d'étude pour élaborer les procédés de production industriels : définir les responsabilités et tâches de chaque service, réunions de suivi des travaux...
9. Veille technologique	<ul style="list-style-type: none">Être sûr que l'organisation identifie rapidement les technologies pouvant permettre de développer de nouveaux produits, d'améliorer ses anciens produits, d'améliorer son outil de production et sa productivité.	<ul style="list-style-type: none">Aucune information recensée sur les nouveautés technologiques ou information indisponible.Aucune personne réellement en charge ou formée à ce type de démarche de veille.	<ul style="list-style-type: none">Liste des habilitations des personnes qui sont responsables de cette mission.Procédures de sélection et de tri des informations.Origine des informations/sources.Procédure de hiérarchisation de priorités et/ou de sélection des informations.	<ul style="list-style-type: none">Ne pas identifier une innovation majeure.Perte de part de marché : les concurrents développent des produits plus avancés.Temps de réaction trop long.	<ul style="list-style-type: none">Établir une procédure de veille technologique.Préciser les habilitations et rôles de chacun dans le processus de veille technologique.Établir des procédures de sélection et de hiérarchisation en termes de priorité des informations.Interface R&D et services concernés (production, marketing) afin de faciliter les remontées d'informations sur les tendances, sur le contenu technologique des produits concurrents, et assurer une consultation permanente.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
1. Connaissance du marché et de son environnement	<ul style="list-style-type: none">Être sûr que le marché et ses évolutions sont parfaitement connus et maîtrisés par le service marketing.	<ul style="list-style-type: none">Absence ou insuffisance d'informations nécessaires à une bonne connaissance du marché (pas d'étude de marché).Position actuelle dominante ne favorisant pas la sensibilisation des services concernés à ce type de préoccupations.	<ul style="list-style-type: none">Études de marchés, Documents d'analyse du cycle de vie des produits.Étude régulière des facteurs d'évolution des marchés (conjoncture économique, politique ou sociale, variations saisonnières, modes, temps, offres, environnement).	<ul style="list-style-type: none">Perte de chiffre d'affaires, de parts de marché.Non-atteinte des objectifs commerciaux.Manque de réactivité de l'organisation face à de nouvelles opportunités.Perte d'image vis-à-vis de la clientèle actuelle.	<ul style="list-style-type: none">Formaliser les étapes de réalisation des études de marchés.Disposer de toutes les données nécessaires à la détermination de la taille du marché (CA du marché, nombre d'acheteurs, quantité moyenne par acheteur, ventes totales, taux de pénétration, valeur d'un consommateur).Faire un point régulier sur les tendances actuelles et futures du marché (structure du marché, évolutions...) et sur le positionnement de l'organisation.Mise à jour des techniques relatives aux études de marché.Faire une veille technologique périodiquement afin de prendre en compte les avancées technologiques dans les études de marché.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
	– Être sûr que la concurrence est connue et maîtrisée par le service marketing (opportunités de développement et/ou menaces de mise en péril de certains produits ou services proposés par l'organisation).	– Concurrents mal identifiés. – Absence ou insuffisance en matière de veille concurrentielle (documentations nécessaires, compétences requises...) – Position actuelle dominante ne favorisant pas la sensibilisation des services concernés à ce type de préoccupations.	– Documents d'analyse de la position concurrentielle et calcul des parts de marché. – Sources diverses en matière de veille concurrentielle.	– Perte de chiffre d'affaires, de parts de marché. – Non-atteinte des objectifs commerciaux.	– Formaliser les étapes de réalisation des analyses concurrentielles. – Définir les critères permettant une analyse complète de la position concurrentielle (position sur le marché, puissance de la marque, critères techniques, critères financiers, modes de calcul des parts de marché en volume et en valeur...) – Diversifier les sources en matière de veille concurrentielle (clients, distributeurs, fournisseurs, prestataires, panel, presse, salons, colloques, informations financières publiées, déclarations, études...).
	– Être sûr que les besoins des consommateurs et les facteurs influençant l'achat ont bien été identifiés.	– Absence ou insuffisance d'analyse comportementale des consommateurs. – Outils de veille (quantitatifs et qualitatifs) inadaptés.	– Analyse des principaux facteurs influençant l'achat. – Sources d'informations sur les besoins actuels et besoins futurs (statistiques, comptes rendus de la force de vente, sondages...).	– Perte de chiffre d'affaires, de parts de marché. – Perte d'image vis-à-vis de la clientèle actuelle. – Insatisfaction des clients. – Perte financière.	– Définir les facteurs influençant l'achat : facteurs socioculturels, psychosociaux, personnels, psychologiques (besoins, motivation, perception, apprentissage, attitudes). – Vérifier l'existence d'études prévisionnelles des débouchés d'un produit ou service.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
2. Choix des options stratégiques fondamentales	Segmentation – Être sûr que le marché a été découpé en sous-ensembles aussi homogènes que possible, afin de permettre à l'organisation d'adapter au mieux sa politique marketing à chacun de ces sous-ensembles, ou à certains d'entre eux.	– Mauvaise connaissance du marché. – Critères de segmentation non pertinents, difficilement mesurables, non pratiques ou non mesurables par le marketing.	– Procédure de segmentation. – Documents d'analyse statistique des différences entre segments.	– Faible rentabilité. – Perte de parts de marché.	– Vérifier l'existence de procédures de segmentation. – Vérifier la pertinence des choix de segments. Les critères doivent être choisis <i>a priori</i> et confirmés par des analyses statistiques des différences entre segments.
	Ciblage – Être sûr que l'attrait relatif de chaque segment a été évalué afin de déterminer au mieux le choix des cibles.	– Les segments choisis ne sont pas assez importants pour être rentables. – Segment trop perméable et ouvert à la concurrence. – L'entreprise n'a pas la capacité matérielle et financière pour entrer sur le marché.	– Études de marché par segments. – Documents d'analyse interne évaluant la capacité de l'entreprise à entrer sur un marché.	– Cibles non atteintes. – Faible rentabilité. – Perte de parts de marché.	– Définir des prévisions chiffrées et détaillées permettant de déterminer la rentabilité future du segment choisi. – Mener des analyses de la concurrence par segment. – Faire un point sur les caractéristiques de l'entreprise (moyens matériels et financiers) pour déterminer son aptitude à toucher le segment ciblé.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
	Positionnement – Être sûr que le public puisse situer le produit dans l'univers des produits analogues et le distinguer des autres.	– Absence ou insuffisance d'informations sur les produits concurrents. – Le produit n'est pas clairement identifié. – Le produit n'est pas différencié des autres du même genre.	– Analyse des attentes du public. – Analyse du positionnement des concurrents. – Étude d'image ou de concept pour déterminer les atouts potentiels du produit.	– Positionnement du produit inadapté. – Faible taux de vente.	– Définir le positionnement du produit (service marketing). – Mener des analyses des attentes du public, du positionnement des concurrents et d'études d'image ou de concept.
3. Formulation et évaluation du marketing mix	Produit – Être sûr que le produit a été clairement et stratégiquement défini.	– Informations sur les attributs clés du produit inexistantes ou approximatives. – Cible et positionnement incohérents, pas clairs. – Aucune information des normes en vigueur. – Mauvaise hiérarchisation des critères prioritaires des consommateurs.	– Étude des attributs clés jouant un rôle majeur dans les perceptions et attitudes des consommateurs. – Règles communes de fabrication et de présentation des produits.	– Faible taux de vente. – Pas de garantie sur le système de qualité du produit. – Menace d'exclusion du marché. – Pas de retour sur investissement.	– Formaliser une procédure claire et complète sur l'aspect produit : définition (produit et attributs, norme, gamme, conditionnement et emballage, service, marque) et cycle de vie du produit. – Mener des études de marché afin de déterminer le produit le plus attractif possible auprès des consommateurs. – Établir des règles communes de fabrication et de présentation des produits (normes). – Vérifier l'adéquation du produit avec le budget et les technologies alloués au projet par l'entreprise. – S'assurer que le service marketing travaille en relation avec le service R&D pour l'élaboration de nouveaux produits.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	Produit – Être sûr que le produit possède un fort potentiel pour l'avenir.	– Les moyens possédés par l'entreprise ne permettent pas de réaliser le service et/ou le produit. – Mauvaise analyse du marché. – Lancement d'un produit sur un segment non viable ou en décroissance.	– Estimation du cycle de vie du produit. – <i>Benchmark</i> auprès des concurrents. – Informations sur le secteur du produit (image, pérennité, etc.).	– Pas de retour sur investissement. – Menace d'exclusion du marché. – Faible taux de vente. – Mise en péril de la pérennité de l'entreprise.	– Mener des études de marché afin de déterminer le produit le plus attractif possible auprès des consommateurs. – Déterminer la place du produit dans son cycle de vie. – Effectuer des démarches sur le segment de marché des produits.
	Prix – Être sûr que le prix a une influence positive sur la rentabilité de l'entreprise et ne constitue pas une barrière à l'achat pour les consommateurs.	– Mauvaise évaluation du coût de production, du prix de revient, des prix des concurrents et des distributeurs. – Le prix n'est pas cohérent avec le positionnement du produit ou du service. – Le public visé ne correspond pas à la gamme de prix choisie.	– Procédures de fixation des prix. – Études des coûts de production. – Documents de <i>benchmarking</i> axé sur le prix des concurrents. – Étude de l'élasticité de la demande finale par rapport au prix.	– Faible taux de vente. – Insatisfaction des clients. – Perte de parts de marché. – Diminution du CA (rentabilité 0).	– Formaliser les modalités de prise en compte des 4 facteurs suivants pour la détermination du prix : objectifs généraux de la stratégie marketing, structure des coûts de production, politique de prix des concurrents et distributeurs, élasticité de la demande finale par rapport au prix. – Vérifier l'adéquation entre le prix de vente, le prix de revient, la stratégie de vente et le positionnement du produit face aux consommateurs. – Définir les modalités de collaboration entre le service marketing, le service commercial, le contrôle de gestion et les autres services financiers.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	Distribution – Être sûr que les canaux de distribution retenus sont cohérents avec la stratégie adoptée concernant le produit ou service à vendre.	– Méconnaissance des différents circuits de distribution.	– Études réalisées concernant les circuits de distribution pertinents en fonction du produit. – Canaux de distribution utilisés. – Enquêtes de satisfaction des différents intermédiaires. – Délais de distribution.	– Perte de clients potentiels. – Perte de CA. – L'image et le positionnement du distributeur ne sont pas en adéquation avec le produit. – Mauvais approvisionnement.	– Mener une étude prenant en compte les caractéristiques du produit, des intermédiaires et de l'environnement afin de déterminer un choix cohérent des circuits de distribution.
	Publicité – Être sûr que la communication sur le produit est faite en adéquation avec le public visé.	– Mauvaise connaissance de l'audience par l'émetteur. – Mauvaise répartition du budget entre les outils de communication.	– Études réalisées sur les populations ciblées. – Plan et budget de communication (annonces presse, spots radio, messages télévisés...). – Dispositifs de fidélisation client.	– Le message n'est pas décodé ou pas entendu par le récepteur. – Faible taux de vente. – Perte de clients potentiels.	– Mener des analyses des populations ciblées et de leur rapprochement avec le produit et le mode de promotion choisi. – Établir et faire valider le plan média par la direction.
	Promotion – Être sûr que les moyens utilisés pour promouvoir le produit sont pertinents et efficaces.	– Moyens de promotion du produit inadaptés. – Mauvaise répartition du budget entre les outils de communication.	– Répartition des budgets promotion par rapport aux objectifs. – Études concernant le rapprochement entre positionnement du produit, cible et moyens de promotion.	– Pas de retour sur les investissements en communication. – L'organisation ne parvient pas à faire connaître son produit. – Faibles ventes et hausse des stocks.	– Définir un plan et un budget de communication. – Effectuer le rapprochement entre le contenu de chaque partie du plan média avec les différents objectifs.

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
4. Planification	<ul style="list-style-type: none">Être sûr que les objectifs marketing définis sont déclinés au niveau opérationnel en plan d'actions.	<ul style="list-style-type: none">Stratégie marketing floue (cible, positionnement, ventes...).	<ul style="list-style-type: none">Objectifs stratégiques.Plans d'action (nature des opérations à mener, responsabilités et moyens nécessaires...).	<ul style="list-style-type: none">Absence de réalisation des objectifs stratégiques, s'ils ne sont pas déclinés et affectés.	<ul style="list-style-type: none">Définir des plans d'action cohérents avec la stratégie marketing, qui soient validés par la DG et les services concernés (commercial, production, R&D...).Attribuer les plans d'actions détaillés à des personnes responsables de leur réalisation dans les délais impartis (et leur affecter les moyens nécessaires).
5. Mise en œuvre	<ul style="list-style-type: none">Être sûr de la bonne réalisation des plans d'action sur le terrain par les personnes et/ou les services concernés.	<ul style="list-style-type: none">Absence de plans d'action ou plans d'action flous, sans responsable identifié.Moyens insuffisants pour la mise en œuvre des plans d'action.Plans d'action non validés avec les autres services concernés.	<ul style="list-style-type: none">Moyens de communication des plans d'action aux services concernés (production, finance, commercial, RH...) et réunions de travail pour suivre leur bonne mise en œuvre.Outils de pilotage de l'avancement des plans d'action.Liste des personnes en charge de ce pilotage.	<ul style="list-style-type: none">Non-atteinte des objectifs et des plans d'action.Résistance des autres services pour la mise en œuvre des plans d'action.	<ul style="list-style-type: none">Effectuer un suivi de la mise en œuvre des plans d'action (de la réunion de lancement au bilan) régulier et avec l'ensemble des acteurs concernés.Mettre en œuvre un système de communication adapté entre les services.Mettre en œuvre un système de remontée des informations pertinentes vers les personnes en charge du pilotage (DG...).

PROCESSUS ET/OU DOMAINE : marketing					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle					
(découpage du processus et/ou domaine de gestion)					
6. Contrôle et veille	<ul style="list-style-type: none">– Être sûr que les résultats des actions marketing sont mesurés afin d'en apprécier l'efficacité et qu'ils servent au pilotage de l'activité (actions correctives en cas de dérive, identification des opportunités à saisir...).– Être sûr que le dispositif de contrôle couvre l'ensemble des risques.	<ul style="list-style-type: none">– Contrôle discontinu.– Planification n'ayant pas intégré de dispositifs de contrôle des actions.– Absence d'objectifs chiffrés dans les plans d'action.– Outils de contrôle ne permettant pas d'évaluer les objectifs.– Absence de moyens nécessaires à la veille technologique.	<ul style="list-style-type: none">– Dispositifs de contrôle dans les plans d'action.– Outils de contrôle disponibles pour évaluer les objectifs : existence et cohérence.– Réalisation effective des contrôles.– Dispositifs de veille concurrentielle (existence et modalités de fonctionnement).– Comparer le résultat avant et après les actions correctives.	<ul style="list-style-type: none">– Objectifs marketing non atteints.– Perte financière directe et indirecte.– Perte de clients et de parts de marché.	<ul style="list-style-type: none">– Définir les dispositifs de contrôle et de pilotage concernant la mise en œuvre des actions marketing au regard des objectifs commerciaux.– Anticiper les écarts en mettant en place des mesures correctives influant sur les objectifs ou les moyens d'action.– Mise en œuvre d'un système de veille concurrentielle continu permettant une réactivité de l'organisation par rapport aux évolutions de son environnement.

PROCESSUS ET/OU DOMAINE DE GESTION : achats						
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			Impacts	EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Activités de contrôle		
1. Expression du besoin	<ul style="list-style-type: none">Être sûr que l'achat correspond à un besoin réel de l'organisation et qu'il est validé par une personne autorisée.	<ul style="list-style-type: none">Achat non nécessaire, non réalisable ou non autorisé.Achat non conforme aux principes de l'organisation.Achat inutile ou non anticipé.Achat d'urgence non maîtrisé.	<ul style="list-style-type: none">Organigramme détaillé avec définitions de fonction écrites pour la demande d'achat (DA) et son acceptation.Règles et pouvoirs de signature.	<ul style="list-style-type: none">Achat mal défini risquant de ne pas correspondre aux besoins.Risque de dépassement par rapport au budget.	<ul style="list-style-type: none">Mettre à jour régulièrement la hiérarchisation des pouvoirs au niveau des DA qui sera émise par un responsable du service demandeur et validées par une personne autorisée.Valoriser et référencer la DA à un budget.Référencer la DA à un cahier des charges pour certains types d'achats.Mettre en place une procédure d'exception pour les achats en urgence (si récurrence de ce type d'achat).	
2. Sélection du fournisseur	<ul style="list-style-type: none">Être sûr d'obtenir un maximum d'informations sur les fournisseurs potentiels afin d'évaluer leurs propositions équitablement et ainsi comparer leurs offres de manière pertinente.	<ul style="list-style-type: none">Fournisseurs potentiels non consultés.Fournisseurs privilégiés.Absence de véritable mise en concurrence.Mauvaise évaluation du fournisseur sélectionné par des critères de comparaison inadéquats (éléments quantifiables : prix, délai, qualité et fiabilité).Absence de cahier des charges précis définissant les besoins.Absence d'appels d'offres.	<ul style="list-style-type: none">Annuaire professionnels.Offres fournisseurs.Fiches fournisseurs.Procédure d'appels d'offres (AO).Procédure de dépouillement des offres.Pertinence, fiabilité et qualité du système d'information fournisseurs.Procédure de qualification des fournisseurs.	<ul style="list-style-type: none">Fournisseurs ne répondant pas aux attentes (rupture des approvisionnements).Surcoût des achats par absence véritable de mise en concurrence.Collusion.Fournisseurs ne respectant pas les réglementations en vigueur.	<ul style="list-style-type: none">Mettre en place un système d'information sur les fournisseurs à la disposition des acheteurs.Supprimer les relations de dépendance avec les fournisseurs.Mettre en place une procédure d'AO (pour les montants dépassant un seuil défini par l'entreprise) et de dépouillement (par le service achats et le service demandeur).L'acheteur doit rédiger l'AO en collaboration avec les demandeurs après étude préalable du marché.Définir des critères de comparaison permettant de justifier les choix (prix, qualité, technicité des produits, situation du fournisseur, sa capacité à respecter les délais et les principes éthiques de l'entreprise).Existence d'une procédure pour évaluer périodiquement les fournisseurs.	

PROCESSUS ET/OU DOMAINE DE GESTION : achats					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
3. Négociation et contrat	<ul style="list-style-type: none">Être sûr que les commandes existent et que les termes de ces commandes ont été négociés, formalisés et autorisés.	<ul style="list-style-type: none">Termes de la commande non négociés.Termes de la commande négociés mais non formalisés.Engagement non autorisé.Court-circuitage par le service demandeur de la procédure d'achat.	<ul style="list-style-type: none">Règles et pouvoirs de signature.Liste de fournisseurs autorisés.Bons de commande (BC).Accusés de réception de commande (AR).	<ul style="list-style-type: none">Non-respect des termes de la commande.Termes de la commande modifiés à des fins personnelles.Litiges avec les fournisseurs.Achats non conformes aux principes de l'entreprise.Dépassement par rapport au budget.	<ul style="list-style-type: none">Mettre en place un support de commande standard numérotée et comportant les conditions générales d'achat (conditions de transport, conditions de paiement...).Mettre à jour régulièrement la liste des personnes habilitées à signer les commandes.Diffuser l'information de la passation de commande au service demandeur, au service comptabilité et au service réception.Vérifier la conformité du contrat aux termes de la négociation.Sécuriser les termes du contrat liés à la propriété intellectuelle.
4. Suivi des commandes en cours	<ul style="list-style-type: none">Être sûr que les commandes en cours font l'objet d'un suivi fiable, pertinent et efficace.	<ul style="list-style-type: none">Absence d'un suivi des engagements de l'entreprise.Absence d'une procédure de suivi des commandes en cours ou procédure incomplète ou imprécise.	<ul style="list-style-type: none">Bons de commande (BC).Accusés de réception de commande (AR).Tableau de suivi des commandes en cours.	<ul style="list-style-type: none">Non-respect des termes de la commande.Risque de litiges importants (non-respect des délais de livraison).	<ul style="list-style-type: none">Diffuser l'information de la passation de commande au service demandeur, au service comptabilité et au service réception.Classer les BC en attente de réception et AR.Rapprocher les BC avec les AR.Établir un tableau de suivi des commandes en cours.

PROCESSUS ET/OU DOMAINE DE GESTION : achats					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
5. Réception des marchandises ou livraison de la prestation	<ul style="list-style-type: none">– Être sûr que le contrôle de la réception des marchandises ou de la livraison de la prestation est correctement effectué de façon à vérifier la conformité avec la commande.	<ul style="list-style-type: none">– Méconnaissance des livraisons.– Absence d'une procédure de contrôle ou procédure incomplète ou imprécise.– Bons de commandes (BC) et/ou bons de livraison (BL) « égarés ».– Absence de rapprochement entre BL et marchandises reçues.	<ul style="list-style-type: none">– Bons de commande (BC).– Bons de livraison (BL).– Bons de réception (BR).– Lettres de relance, réclamation aux fournisseurs.– Bordereaux de retour.	<ul style="list-style-type: none">– Non-conformité en quantité ou en qualité.– Marchandises reçues ne correspondant pas aux besoins au niveau quantité et/ou qualité.– Ralentissement de l'activité.– Vol de marchandises.– Erreur d'imputation et/ou erreur d'affectation dans les états financiers.	<ul style="list-style-type: none">– Réceptionner les livraisons en des lieux définis.– Établir des bons de réception (BR) et les rapprocher aux BL et BC.– Si des écarts ou des retards sont constatés, relancer le fournisseur et avertir les demandeurs.– Envoyer un double du BR au service comptable et classer l'original en attente de facture (l'enregistrement du BR vaut un bon à payer).– Mettre en place une procédure formalisée concernant les litiges (avec ou sans retour, réclamations).– Veiller au principe de bonne séparation des tâches au niveau de la réception des marchandises.

PROCESSUS ET/OU DOMAINE DE GESTION : achats					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
6. Contrôle et enregistrement des factures, paiement des fournisseurs	<ul style="list-style-type: none">Être sûr que les factures fournisseurs sont correctement contrôlées, enregistrées et réglées.	<ul style="list-style-type: none">Absence de procédure de réception des factures ou procédure imprécise.Procédure de réception des factures méconnue ou mal communiquée.Perte de factures.Absence de rapprochement entre facture et BR (quantité, qualité) et BC (prix).Absence de procédure de paiement des factures ou procédure imprécise.Procédure de paiement des factures méconnue ou mal communiquée.Factures non envoyées au service comptable.Conditions de paiement non définies ou imprécises dans le contrat.Absence de suivi des comptes fournisseurs.	<ul style="list-style-type: none">Factures.Bons de réception (BR).Bons de commande (BC).Mouvements comptes fournisseurs et flux de trésorerie dans les états financiers.Liste de personnes habilitées à signer les documents de paiement.Procédures de réception et de paiement des factures et documents associés.Pratiques au niveau du suivi des dettes fournisseurs.	<ul style="list-style-type: none">Retard ou omission dans la comptabilisation.Problème de <i>cut-off</i> (non-respect des règles comptables de séparation des mois/années).Double paiement.Paiement non autorisé.Factures impayées.Détournements (non-séparation des fonctions).	<ul style="list-style-type: none">Définir, formaliser et communiquer des procédures de réception et de paiement des factures claires et précises en définissant le rôle et les responsabilités de l'ensemble des acteurs (opérations de règlement effectuées différentes de celles qui approuvent les pièces justificatives, comptabilisent les opérations d'achat et paient les règlements bancaires).Mettre à jour la liste des personnes habilitées à signer les documents de paiement.Contrôler systématiquement la facture : aspect formel de la facture correct, date récente et calculs exacts, rapprochement de la facture avec le BR et le BC.Comptabiliser uniquement au vu du justificatif.Analyser périodiquement les comptes fournisseurs et comptes de trésorerie.

PROCESSUS ET/OU DOMAINE DE GESTION : achats					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
7. Gestion de la base informatique « Fournisseurs »	<ul style="list-style-type: none">– S'assurer que la base informatique « Fournisseurs » ne peut pas être modifiée par des personnes non autorisées de manière frauduleuse.– S'assurer que la base « Fournisseurs » n'est pas erronée.	<ul style="list-style-type: none">– Modifications sensibles demandées par des tiers non habilités.– Saisies erronées ou incomplètes des données fournisseurs.	<ul style="list-style-type: none">– Vérification des modifications d'informations.– Sécurisation des données bancaires du fournisseur.– Revue de la base « Fournisseurs » par le responsable des achats.	<ul style="list-style-type: none">– Paiements à des bénéficiaires erronés ou fictifs.– Fraude.	<ul style="list-style-type: none">– Toute création de données sensibles de la base « Fournisseurs » doit être opérée sous supervision formalisée d'une tierce personne ne disposant pas d'habilitation pour modifier la base.– Toute demande de modification de données sensibles « Fournisseurs » doit être vérifiée et confirmée (contre-appel...).– Mise à jour périodique des habilitations de création/modification de la base « Fournisseurs ».– Désactivation des fournisseurs inactifs depuis une période prolongée.
8. Implication du service achats dans le pilotage du groupe	<ul style="list-style-type: none">– Être sûr que le service achats participe à l'élaboration du budget annuel et des plans d'achats annuels.	<ul style="list-style-type: none">– Non-prise en compte des stocks lors de l'élaboration du budget achats.– Le service achats ne participe pas à l'élaboration de son budget et des plans d'achats.	<ul style="list-style-type: none">– Analyse des écarts précédents entre le prévisionnel et le réel.– Procès-verbal de la réunion d'élaboration du budget.– Planning budgétaire des dépenses.– Prévisions des évolutions de stocks.	<ul style="list-style-type: none">– Prévisions de budget en déconnexion avec les objectifs et les contraintes opérationnelles de l'activité.– Absence de maîtrise des coûts.	<ul style="list-style-type: none">– Impliquer le service achats dans l'élaboration du budget annuel, des plans d'achats annuels et des écarts prévisions/réel.– Établir un planning des principales commandes passées par le service.– Prendre en compte les états de stocks lors de l'élaboration des budgets achats.

PROCESSUS ET/OU DOMAINE DE GESTION : achats					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">– Être sûr que le service achats est l'interlocuteur privilégié des fournisseurs.	<ul style="list-style-type: none">– Absence de contact des achats avec l'extérieur : faible autonomie.– Éclatement de la fonction achat en pôles autonomes.– Court-circuitage de la fonction achat par les clients internes.– Contrats signés au coup par coup.– Pratique de commande trop pointilleuse remettant en cause le partenariat à chaque commande.	<ul style="list-style-type: none">– Nomenclature des fournitures et matériels.– Procédure achat et post-achat.– Délégations de signature et circuit de validation.– Contrats fournisseurs.– Éléments d'évaluation des fournisseurs.	<ul style="list-style-type: none">– Détérioration des rapports avec les fournisseurs.– Diminution de la crédibilité du service achats et donc de son poids décisionnel.	<ul style="list-style-type: none">– Ratifier des contrats de longue durée avec les principaux fournisseurs.– Bon maintien des relations avec les fournisseurs.– Donner au service achats une autonomie importante en termes d'évaluation des fournisseurs.– Rendre l'approbation officielle du service achats obligatoire pour toute commande.

PROCESSUS ET/OU DOMAINE DE GESTION : gestion des stocks					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
1. Estimation et prévision des stocks	– Être sûr que le stock permettra de satisfaire les aléas de la demande des clients (externe/interne).	– Stocks insuffisants pour la production. – Absence de mise à jour des caractéristiques de l'appareil productif.	– Prévision des ventes/objectifs généraux. – Procédure d'estimation des stocks. – Rapprochement avec inventaires périodiques. – Tableaux de gestion des stocks par produit. – Planning des demandes de sorties en provenance des services clients.	– Suresimation du stock nécessaire, risque de charges financières supplémentaires. – Sous-évaluation du stock nécessaire, risque de rupture de stock. – Apparition de stocks dormants.	– Estimation des besoins en stock en collaboration avec les services contrôle de gestion/marketing/commercial/production. – Mise à jour des caractéristiques de l'appareil productif à chaque modification du processus de production. – Effectuer des inventaires périodiques afin d'estimer les niveaux de stocks en vue d'ajuster les prévisions.
	– Être sûr que l'estimation des niveaux de stocks nécessaires tient compte du stock de sécurité et correspond à l'activité de l'organisation.	– Absence de procédure d'estimation des stocks. – Les stocks de sécurités ne sont pas connus. – Présence de stocks dormants non pris en compte. – Absence de méthode précise d'estimation des stocks. – Pas de prise en compte des contraintes techniques liées aux produits, aux matières ou à l'activité.	– Procédure d'estimation des stocks. – Données historiques (niveau de production/stocks des années précédentes). – Travaux d'estimation des stocks nécessaires. – Instructions de gestion des stocks. – Typologie des produits. – Instruction sur les niveaux de stocks de sécurité tolérés. – Tableaux de gestion des stocks par produit.	– Suresimation du stock nécessaire, risque de charges financières supplémentaires. – Sous-évaluation du stock nécessaire, risque de rupture de stock. – Apparition de stocks dormants.	– Estimation des besoins en stock en collaboration avec les services contrôle de gestion/marketing/commercial/production. – Mise à jour des caractéristiques de l'appareil productif à chaque modification du processus de production ou à sa modification. – Ajuster les prévisions de stockage en fonction des stocks existants. – Effectuer des inventaires périodiques afin d'estimer les niveaux de stocks en vue d'ajuster les prévisions. – Prendre en compte les contraintes techniques d'approvisionnement lors de l'élaboration des plannings de réapprovisionnement.

PROCESSUS ET/OU DOMAINE DE GESTION : gestion des stocks					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
2. Les mouvements de stock (entrées/sorties)	– Être sûr que tout mouvement de stock correspond à une réalité et a une justification.	– Entrée ou sortie de stock fictive. – Absence de bon de cession au client/demandeur. – Absence de rapprochement entre liste des commandes et entrées en stock. – Absence de suivi entrées/sorties.	– Fiche des entrées/sorties de stocks. – Liste des bons de cessions. – Liste des commandes. – Liste des bons de réception. – Liste des bons d'expédition.	– Risque de démarque (dédoublement de stocks). – États financiers faussés. – Charges financières supplémentaires. – Accroissement des volumes de stocks de façon non justifiée.	– Signature du bon de réception par le service gestion des stocks et le service achats. – Procédure entrées et sorties de stocks. – Rapprochement bon de commande du client/bon de livraison/bon de réception client. – Rapprochement bon de réception du service/bon de commande de la société.
	– Être sûr que tout mouvement de stock est enregistré.	– Non-enregistrement des mouvements de stocks. – Absence de dispositif de tracking des produits. – Dispositif de tracking non uniforme.	– Procédures d'entrées et sorties de stock. – Récapitulatif des entrées/sorties journalières comparé au stock net en fin de journée.	– Charges financières supplémentaires. – États financiers faussés.	– Tracer les produits de façon homogène via le même dispositif. – Enregistrer les mouvements de stocks en temps réel.
	3. Maintien du niveau de stock et réapprovisionnement	– Être sûr que, pour tout besoin de reconstitution des stocks, un réapprovisionnement est fait.	– Absence de commande systématique en deçà d'un certain niveau de stock. – Stock de sécurité calculé erroné. – Délais de réapprovisionnement trop longs.	– Estimation d'une marge de stockage correspondant aux aléas de la demande. – Estimation du niveau de stock nécessaire. – Listing des arrivées de réapprovisionnement. – Liste des demandes de réapprovisionnement rapprochée au niveau de stock actuel. – Méthode de calcul du seuil de réapprovisionnement.	– Rupture de stock. – Surfacturations des fournisseurs/prestataires logistiques. – Estimation des stocks erronée, ce qui biaise les informations financières. – Coût de réapprovisionnement trop important.

PROCESSUS ET/OU DOMAINE DE GESTION : gestion des stocks					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr que le niveau de stock est maintenu.	<ul style="list-style-type: none">Mauvaise estimation des niveaux de stocks.	<ul style="list-style-type: none">Méthode de calcul du seuil de réapprovisionnement.Estimation du niveau de stock nécessaire.États des ruptures de stock.	<ul style="list-style-type: none">Perte de contrat (ou litige).Ruptures de stock.Impossibilité à satisfaire une commande.Charges financières éventuelles (pénalité de retard, absence de négociation des tarifs due aux petites quantités).	<ul style="list-style-type: none">Mise en place d'un outil de réapprovisionnement automatique en deçà d'un certain niveau de stock.Suivre une méthode de calcul unique pour toute définition des seuils de réapprovisionnement.
4. Évaluation / valorisation des stocks	<ul style="list-style-type: none">Être sûr que le stock est évalué selon les principes comptables de l'organisation.	<ul style="list-style-type: none">Défaut de connaissance des normes comptables choisies par l'entreprise/le groupe pour la valorisation des stocks (CUMP, etc.).Absence de méthode de valorisation des stocks.Valorisation des stocks hétérogène en fonction de la période.	<ul style="list-style-type: none">Communication des normes comptables de l'entreprise/du groupe.Procédure de valorisation des stocks et des en-cours.Fiche de suivi des stocks.États de valorisation des stocks des années précédentes.	<ul style="list-style-type: none">Valorisation comptable des stocks faussée, états financiers faussés (BFR, provisions, etc.).Baisse de crédibilité.Prise de décision éventuellement erronée.	<ul style="list-style-type: none">Mettre en place une procédure de valorisation des stocks en accord avec les règles comptables de la société/du groupe, procédure incluant les en-cours.Nommer un responsable de la valorisation des stocks.Réaliser une valorisation périodique en rapprochant les sorties (et demandes des services) et les entrées en stocks (réception de marchandise).

PROCESSUS ET/OU DOMAINE DE GESTION : gestion des stocks					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">– Être sûr que la valorisation est représentative de la réalité.	<ul style="list-style-type: none">– Outil/méthode de valorisation non efficace.– La valorisation n'est pas effectuée au moment opportun.	<ul style="list-style-type: none">– Procédure de valorisation des stocks et des en-cours.– Rapprochement des valeurs des références stockées sur site avec les valeurs estimées sur le marché.	<ul style="list-style-type: none">– Baisse de crédibilité.– Prise de décision éventuellement erronée.– Risque de non-certification des comptes et/ou de redressement fiscal.	<ul style="list-style-type: none">– Mettre en place une procédure de valorisation des stocks en accord avec les règles comptables de la société/du groupe, procédure incluant les en-cours.– Nommer un responsable de la valorisation des stocks.– Réaliser une valorisation périodique en rapprochant les sorties (et demandes des services) et les entrées en stocks (réception de marchandise).
5. Inventaire des stocks	<ul style="list-style-type: none">– Être sûr que le résultat de l'inventaire des stocks est conforme à la réalité.	<ul style="list-style-type: none">– L'inventaire n'est pas exhaustif.– Absence de procédure d'inventaire.– Absence ou mauvaise séparation des tâches.– Absence de plan/programme d'inventaire.	<ul style="list-style-type: none">– Procédure d'inventaire des stocks incluant la séparation des tâches.– Fiche(s) d'inventaire(s).– Plan/programme d'inventaire.– Liste du personnel d'inventaire.– Dispositif de sécurité physique.	<ul style="list-style-type: none">– États financiers faussés.– Risques de démarque (détournement de stocks).	<ul style="list-style-type: none">– Procédure d'inventaire physique exhaustive.– Séparation des tâches.– Événuel double comptage pour les stocks critiques ou en cas d'écarts.– Contrôles de l'inventaire.– Plan/programme d'inventaire.– Faire effectuer, par une personne n'ayant pas participé à l'inventaire physique, un rapprochement entre les stocks virtuels (dans le SI) et les stocks réels.– Sécuriser les accès de l'entrepôt lors du déroulement de l'inventaire.

PROCESSUS ET/OU DOMAINE DE GESTION : gestion des stocks					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr que l'organisation des inventaires physiques assure une continuité d'exploitation.	<ul style="list-style-type: none">Absence ou mauvaise séparation des tâches.Manque de ressources nécessaires lors de l'inventaire.	<ul style="list-style-type: none">Date de l'inventaire.Plan/programme d'inventaire.	<ul style="list-style-type: none">Pertes financières.Cessation d'activité.	<ul style="list-style-type: none">Procéder à l'inventaire durant les périodes creuses de l'activité.Planifier le déroulement de l'inventaire en corrélation avec l'activité.
6. Sécurisation des stocks	<ul style="list-style-type: none">Être sûr que la sécurité des stocks est assurée.	<ul style="list-style-type: none">Locaux non sécurisés.Absence/non-application de règles de sécurité.Non-restriction de l'accès aux stocks.	<ul style="list-style-type: none">Règles de sécurité.Preuves de l'entretien des systèmes de sécurité.Règlement intérieur.Liste des personnes ayant suivi une formation sécurité.	<ul style="list-style-type: none">Destruction ou détournement des stocks.Charges financières.	<ul style="list-style-type: none">Souscription d'une assurance.Mise à jour des règles de sécurité et communication de celles-ci.Systèmes de prévention/détection/protection entretenus.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
1. Conception et études préalables à la production	– Être sûr qu'on étudie quels seront les concepts technologiques et/ou méthodes à utiliser pour satisfaire le cahier des charges.	– Concurrence avec la fonction R&D. – Technologie trop compliquée à mettre en œuvre. – Coût trop élevé. – Concept en inadéquation avec les besoins des clients.	– Cahier des charges bien suivi. – Communication et collaboration lors de l'élaboration du cahier des charges. – Définition précise des rôles de la R&D et du bureau d'étude. – Connaissance et communication des moyens de production existants et des normes de fabrication.	– Risque de conflits de pouvoir entre fonction R&D et production. – Augmentation des délais de lancement et mise en production. – Difficulté à passer d'un stade de production expérimental à un stade de production industrielle. – Production irréalisable, inadaptée.	– Assurer un suivi strict du cahier des charges. – Communiquer sur les aspects techniques importants de la mise en production ainsi que sur le planning de développement. – Collaboration entre ces deux services. – Veiller à ce que du personnel R&D soit détaché pour aider à la mise en place de la production.
	– Être sûr que ces concepts et/ou méthodes de production sont définis afin de minimiser les coûts, les pertes de temps et de garantir une sécurité maximale.	– Les études réalisées ne suivent pas les mêmes orientations stratégiques que les objectifs de l'entreprise. – Il y a des contradictions dans les études réalisées. – Absence de réunions de travail entre les collaborateurs et/ou les différents bureaux d'étude.	– Budget production validé. – Points de vérification du cahier des charges validés avec le client. – Connaissance et communication des moyens de production existants et des normes de fabrication.	– Augmentation des délais de lancement et mise en production. – Augmentation des coûts due à l'aboutissement sur des solutions non optimisées.	– Prévoir au préalable une estimation du budget de mise en production. – Veiller à la conformité et au caractère réalisable des projets.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	– Être sûr que les études théoriques sont réalisables, cohérentes et qu'elles ne remettent pas en cause les objectifs de l'organisation.	– Absence d'objectifs clairs. – Absence de réunions de travail entre les collaborateurs et/ou les différents bureaux d'étude.	– Réunion périodique d'analyse des études réalisées. – Cahier des charges relatant les exigences que devra respecter l'outil de production. – Existence et connaissance des objectifs organisationnels.	– Les études ne répondent pas aux besoins de l'entreprise. – Augmentation des délais de lancement et mise en production. – Non-conformité des projets avec le cahier des charges.	– Évaluer les écarts entre les études réalisées et les objectifs finaux. – Les études réalisées doivent être orientées dans le même axe que ces objectifs. – Les études doivent aboutir sur des projets réalisables. – Tenir des réunions périodiques permettant de faire un point et de recadrer l'étude en cas de « dérive » par rapport aux objectifs.
	– Être sûr de la bonne coordination entre le service R&D, le bureau d'étude, le service ordonnancement/ lancement.	– Mauvaise connaissance des normes et/ou des moyens de fabrication. – Absence de communication entre les collaborateurs et/ou les différents bureaux d'étude. – Les rôles de la R&D et de la production dans l'élaboration des concepts ne sont pas ou mal définis.	– Cahier des charges relatant les exigences que devra respecter l'outil de production. – Existence et connaissance des objectifs organisationnels. – Réunions de travail périodiques régulières (avancée des travaux).	– Les études ne répondent pas aux besoins de l'entreprise. – Dégradation de l'image de la production auprès des clients interne. – Non-conformité des projets avec le cahier des charges.	– Choix en concertation entre R&D ayant mis au point le produit et bureau d'étude devant gérer la production industrielle de celui-ci. – Définir le rôle de chaque service connexe à la production ainsi que ses moyens (humains et financiers). – Définir la contribution de chaque service aux objectifs opérationnels de la production. – Structurer les études (calendrier...) de façon formelle et les communiquer aux collaborateurs concernés.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
2. Planification de la production	<ul style="list-style-type: none">Être sûr que la production est planifiée de manière à réduire les coûts et les stocks à leur minimum.	<ul style="list-style-type: none">Manque de communication et d'information.La planification est mal effectuée : les prévisions de ventes ne sont pas transformées en prévision de production.Il n'existe aucune méthode formalisée pour arbitrer les priorités de planning.Absence de communication entre les membres du service.Les méthodes de planification ne prennent pas en compte les exigences client.Les délais de planification sont trop courts pour mobiliser les ressources d'appoint.	<ul style="list-style-type: none">Cahier des charges.Plan prévisionnel de production.Système de communication des membres du service.État des stocks.Plans de production passés.Approbation du plan de production.Procédure d'information du service achats des impératifs d'approvisionnement.	<ul style="list-style-type: none">Production en déphasage avec les prévisions de ventes et disponibilité de l'outil industriel.Défaillance de la planification des approvisionnements en termes de quantités ou de délais.Insuffisance ou excédent de matières.Gestion de la production non optimisée.Perte de productivité.Perte de performance.Risque de conflit entre le personnel du service de production.	<ul style="list-style-type: none">Existence de documents standard pour la préparation et la communication des prévisions de ventes et plans de charges.Connaissance des prévisions de ventes et de la disponibilité de l'outil industriel par le personnel de production.Existence de procédures de comparaison des plans de production aux prévisions et d'identification d'écart en termes de délais et de quantités.Établissement de niveaux de priorités au niveau de la production sur la base de critères préétablis.Établissement d'un plan de production annuel précis et réaliste, approbation du plan de production au niveau approprié.Existence d'indicateurs de performance pour suivre les cas d'insuffisance ou d'excédent de stocks de matières.Évaluer la capacité de production de la chaîne de production.Veiller à la formalisation des responsabilités de chacun dans la conception du produit.Mettre en place un système d'information formalisée.Établir un « bon à tirer » pour chaque étape de la production.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	– Être sûr que le service de production respecte le planning budgétaire.	– Le planning budgétaire n'est pas traduisible en exigences de production : trop flou. – Le planning budgétaire se révèle incompatible avec les exigences de la production.	– Budget de production, – Tableau des écarts, – Planning des dépenses liées à la production.	– Gestion de la production non optimisée. – Pertes financières potentielles dues à des dépenses au mauvais moment.	– Communiquer le budget de production au service production. – Intégrer les responsables production dans l'élaboration du budget nécessaire pour respecter le plan de production.
	– Être sûr que chaque membre du service production connaît son rôle.	– Absence de spécialisation dans les tâches. – Pas de rôle défini pour les membres du service production.	– Fiches de poste.	– Risque de conflit entre le personnel du service de production.	– Veiller à la formalisation des responsabilités de chacun dans la conception du produit. – Veiller à ce que chacun respecte sa mission.
	3. Gestion des ressources (travail, capital et matières premières)	– Être sûr qu'une personne gère l'équipe et la dirige vers un but commun. Cette personne est chargée de définir les rôles des membres de l'équipe et de leur attribuer certains pouvoirs.	– Mauvaise définition des rôles. – La distribution des pouvoirs est confuse. – Mauvaise communication entre les postes et le service manutention. – Manque de flexibilité dans la définition de la gestion de la production.	– Organigramme fonctionnel. – Procédures claires et formalisées de transmission des informations. – Plan de travail des équipes. – Aménagements horaires des services par rapport aux cycles de production.	– Conflits engendrant des nuisances pour la société. – Non-atteinte des objectifs. – Diminution de la productivité. – Risque de perte de qualité due à l'accélération de la cadence de production.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr du respect des priorités de production arbitrées au niveau des clients internes : moyens associés à la réalisation du plan de production.	<ul style="list-style-type: none">Définition de moyens non adaptés à la réalisation des objectifs.Contraintes techniques non prises en compte par les clients.Le planning n'est fait que d'urgences.Le plan de production ne prend pas en compte les priorités des clients internes.	<ul style="list-style-type: none">Prévisions de ventes.Plan de production.Attribution des équipes.Spécification technique de la production.	<ul style="list-style-type: none">Retards de production.Insatisfaction clients.Investissements en moyens inadaptés.	<ul style="list-style-type: none">Définition des moyens humains et techniques en relation avec la production et les bureaux des méthodes et d'ordonnancement.Communication des informations rapide et pertinente aux collaborateurs concernés.Suivi des flux en temps réel à l'aide d'outils adaptés.Formaliser une procédure de transmission des informations.Élaborer une liste exhaustive des contraintes techniques de fabrication et la mettre à jour systématiquement : rapprocher les contraintes techniques avec les demandes internes.Mettre en place un système de prise en charge des besoins imprévus.
	<ul style="list-style-type: none">Être sûr que l'approvisionnement des postes de travail, la réception des marchandises des fournisseurs et le rangement des produits finis sont correctement réalisés.	<ul style="list-style-type: none">Manque de matières premières.Seuil limite de ressources mal défini, non connu.	<ul style="list-style-type: none">Seuil minimum de stock.Procédure de réapprovisionnement.Inventaire des moyens mis à disposition de la maintenance.	<ul style="list-style-type: none">Arrêt de la chaîne de production pour ressources insuffisantes.Retard sur la production et l'acheminement aux stocks.Non-atteinte des objectifs.	<ul style="list-style-type: none">Travailler en collaboration avec le service de gestion des stocks et le service d'approvisionnement.Définir clairement le seuil minimum avant approvisionnement.Utiliser des grilles bien définies (dates, quantités) qui informent le service achats des impératifs d'approvisionnement.Comparer les prévisions d'achats avec les achats réels afin de prévoir les quantités de matières premières à utiliser.Répertorier les excédents/insuffisances de stocks de matières premières afin de mieux planifier l'approvisionnement.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	– Être sûr que les stocks de produits finis sont minimisés.	– Seuil limite de ressources mal défini ou non connu. – Manque de clarté dans la définition du plan de fabrication.	– Indicateurs de gestion de stocks. – Commandes clients. – Délais d'attente entre fin de production et expédition.	– Gestion des entrées et sorties de matières non optimale. – Augmentation des charges de stockage. – Diminution du résultat.	– Vérifier le calcul et la prise en compte d'indicateurs. – Attribuer une série produite à une ou plusieurs commandes. – Entretiens réguliers entre le responsable de la gestion des stocks et le personnel du service connexe affecté à cette tâche. – Construction d'indicateurs pertinents.
	– Être sûr que la gestion du stock d'outils nécessaires à la production permet la réalisation des objectifs.	– Absence de calcul d'un seuil de sécurité. – Absence d'informations relatives au niveau des stocks. – Absence de planification. – Mauvaise communication avec le service achats. – Absence de planification des besoins outils et matières premières. – Absence de gestion des stocks outils et ressources.	– Inventaire des moyens mis à disposition de la manutention. – Procédure de gestion du stock d'outils. – Plan de fabrication. – Liste des contraintes techniques.	– Retards dans la production. – Non-atteinte des objectifs. – Continuité de la chaîne de production interrompue.	– Évaluer et suivre les besoins (d'où lancement de la fabrication en interne ou sur commande). – Comparer les méthodes de gestion de la production au niveau coûts/bénéfices afin de mettre en place les meilleurs moyens de gestion des matières premières. – Évaluation et planification des besoins en outils. – Définition des ressources nécessaires au service en collaboration avec les bureaux d'étude, des méthodes et d'ordonnancement. – Évaluer les rapports coût/bénéfice des machines.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">– Être sûr du bon entretien de la chaîne de production et de l'optimisation des coûts et délais d'entretien.	<ul style="list-style-type: none">– Entretien effectué de façon non conforme.– Obsolescence du matériel.– Utilisation non optimale du matériel.– Priorité donnée à la maintenance curative.	<ul style="list-style-type: none">– Planning de maintenance.– Plan de tests.– Guide de diagnostic.– Nomenclature des principales pannes et des réparations associées.– Contrat de prestation.	<ul style="list-style-type: none">– Retards dans la production.– Défaillance du matériel.– Arrêt de production.– Impossibilité de réparer donc matériel inutilisable et obligation de rachat.	<ul style="list-style-type: none">– Diagnostiquer la panne, définir les moyens d'actions et effectuer les actions préventives.– Tester le matériel après les interventions.– Minimiser les périodes d'interruption de la chaîne de production.– Vérifier que la maintenance soit effectuée aux dates prévues.– Vérifier que le matériel soit renouvelé quand cela est nécessaire.– Disposer de contrats de services avec une entreprise de maintenance/ réparation ou avec le fournisseur du matériel.– Entretenir le matériel aux dates prévues par le service de la maintenance.– Vérifier l'existence d'une fiche de produit permettant de situer la défaillance du produit et de son fonctionnement.– Créer une procédure de définition du planning de maintenance.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">– Être sûr que l'outil de production est correctement renouvelé.	<ul style="list-style-type: none">– Dépassement des délais de maintenance.– Utilisation de technologies obsolètes.	<ul style="list-style-type: none">– Planning de maintenance.– Plan de tests.– Cahier des charges.– PV de réunion de projet.– Procédure de mise en fonctionnement de nouveau matériel.– Historique des pannes majeures et solutions de réparation appliquées.	<ul style="list-style-type: none">– Arrêt de production.– Retards dans la production.– Risque de casse anticipée du matériel de production.	<ul style="list-style-type: none">– Sensibiliser le personnel sur la nécessité d'effectuer des tests avant réutilisation du matériel renouvelé.– Mettre en corrélation le cahier des charges concernant le nouvel outil avec les caractéristiques de l'outil renouvelé.– Disposer de contrat de service avec une entreprise de maintenance/ réparation ou avec le fournisseur du matériel.– Entretenir le matériel aux dates prévues par le service de la maintenance.– Formaliser une procédure de vérification avant réutilisation du matériel : check-list des tests à effectuer.– Évaluer le suivi des arrêts de production liés à des défaillances du matériel.
	<ul style="list-style-type: none">– Être sûr de la polyvalence et de la réactivité des ateliers de production.	<ul style="list-style-type: none">– Sous- ou sur-spécialisation du personnel.– Équipes figées.– Postes ne disposant pas de solution de relève.	<ul style="list-style-type: none">– Besoins des clients internes.– Délai moyen de réponse à une commande.– Nombre de litiges clients internes et externes.– Aménagements horaires des services par rapport aux cycles de production.	<ul style="list-style-type: none">– Non-atteinte des objectifs.– Dépendance de la production aux compétences de certains employés.	<ul style="list-style-type: none">– Vérifier que le personnel est formé au travail sur les différents postes de production.– Rendre l'organisation de la production indépendante des salariés qui occupent certains postes.– Mettre en place un système de prise en charge des besoins imprévus.– Former le personnel à travailler sur les différents postes de la chaîne de production.


PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)					
	<ul style="list-style-type: none">Être sûr que les machines répondent aux exigences du service et aux préoccupations de protection de l'environnement.	<ul style="list-style-type: none">Contraintes techniques mal définies, ignorance des lois et règlements, Moyens techniques inadaptés.	<ul style="list-style-type: none">Indicateurs de pannes (informatiques), PV de réunion de projet, Rapport sur la réglementation.	<ul style="list-style-type: none">Non-atteinte des objectifs, Production non conforme aux attentes (cahier des charges non respecté), Non-respect des réglementations (sanction pénale), Risque de perte de qualité, Image de l'entreprise affectée.	<ul style="list-style-type: none">Formaliser un PV pour les réunions de recadrage réglementaire, Mettre en place un dispositif de veille juridique et des réglementations, Élaborer une liste exhaustive des contraintes techniques de fabrication et la mettre à jour systématiquement.
4. Réalisation de la production	<ul style="list-style-type: none">Être sûr que l'on produit et que l'on traite les quantités requises, conformément aux spécifications et aux plans de production.	<ul style="list-style-type: none">Aucun plan de production établi ou plan de production imprécis, Plan de production non ou mal communiqué, Défaillance dans la planification, Incompréhension des étapes du processus de production, Quantités à produire inadaptées ou peu claires, Machines de production inadaptées, Rôles des acteurs non définis ou incompris, Absence de suivi de l'avancement du processus et des résultats obtenus.	<ul style="list-style-type: none">Plan de production, Procédure de production et documents associés, Spécifications de production, Liste des machines (date d'acquisition, capacité de production...), Procédure de traitement des commandes urgentes, Tableau de bord contrôlant le taux de rebuts, Dispositif de sécurité physique des chaînes de production.	<ul style="list-style-type: none">Non-réalisation des objectifs de production, Performance revue à la baisse, retard de production, Perte de temps, d'argent et d'efficacité, Augmentation du taux de rebuts « déchets », Problématiques de recyclage.	<ul style="list-style-type: none">Établir un schéma détaillé décrivant le processus et les méthodes de production, Réaliser un tableau de bord permettant de suivre les résultats de production, l'avancement du processus, le nombre d'heures de travail, les matériaux utilisés et autres..., Connaître le processus de production des concurrents afin de simplifier celui-ci au sein de l'entreprise.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
		ACTIVITÉS DE CONTRÔLE (découpage du processus et/ou domaine de gestion)			
	<ul style="list-style-type: none">Être sûr que la production est réalisée conformément aux lois et réglementations en vigueur en matière d'hygiène et de sécurité, aux normes qualitatifs et obligations légales en matière d'environnement.	<ul style="list-style-type: none">Lois, réglementations, normes non ou mal communiquées, méconnues ou incomprises.Priorités données à la maîtrise des coûts et/ou au respect des délais.Non-respect des normes environnementales.L'outil de production n'est pas aux normes.	<ul style="list-style-type: none">Lois et réglementations en matière d'hygiène et de sécurité.Normes de qualité adoptées par l'entreprise.Normes et obligations légales en matière d'environnement.Système des droits à polluer.Certifications « vertes ».Certificats de maintenance.	<ul style="list-style-type: none">Accidents ou infractions.Problèmes de qualité découverts tardivement.Amendes ou redressement des autorités administratives.Interruption de la production et non-respect des délais.Performance de l'activité revue à la baisse.Impact sur l'image de l'entreprise.	<ul style="list-style-type: none">Création de services de veille « technologique », « juridique »...Sensibilisation et formation du personnel.Procédure de mise à jour et de diffusions des informations.Donner la priorité au respect des lois et normes.Faire certifier la fonction de production à la norme ISO 14001.
5. Assurer la qualité des produits finis	<ul style="list-style-type: none">Être sûr que la production est réalisée conformément aux normes de qualité adoptées par l'organisation.	<ul style="list-style-type: none">Inexistence ou méconnaissance des procédures visant à assurer la qualité des produits.Les problèmes de qualité ne sont pas identifiés durant le processus de production.	<ul style="list-style-type: none">Plan de suivi de la qualité des produits finis.Système de tracking des produits dès leur entrée en chaîne.	<ul style="list-style-type: none">Interruption de la production.Vente de produits défectueux ou de moindre qualité.Perte de clients.Mauvaise image.	<ul style="list-style-type: none">Créer des procédures visant à garantir la qualité du processus de production.Réaliser des tests de contrôle.Sensibiliser le personnel à la maîtrise de la qualité.Établir un indicateur de taux de défauts.Procéder au suivi des retours de marchandises de qualité insuffisante et des réclamations des clients.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
6. Gestion des produits finis	– Être sûr du conditionnement des produits finis.	– Mauvaise transmission des informations. – Manque de personnel. – Manque de temps. – Conditionnement inadapté.	– Contraintes de manipulation des produits. – Procédure de conditionnement/expédition. – Tracking des produits finis. – Normes de transport/manutention (en fonction des produits). – Plannings d'acheminement.	– Dégradation des produits finis. – Pertes financières. – Risque de démarque. – Retards d'expédition.	– Vérifier que les produits finis soient conditionnés conformément aux procédures définies. – Mettre en place des normes de conditionnement. – Séparer les tâches (le personnel qui conditionne est différent de celui responsable de l'acheminement). – Etablir des plannings.
	– Être sûr de l'acheminement vers les stocks.	– Le circuit d'acheminement n'est pas connu. – Le circuit d'acheminement est complexe et implique le passage dans des zones ouvertes sur l'extérieur. – Les moyens et les circuits utilisés pour l'acheminement des produits ne sont pas adaptés. – Manque de temps.	– Itinéraires de transfert chaîne production/stock/expéditions. – Protection physique des circuits d'acheminement ; restriction des accès, marquage au sol... – Contraintes de manipulation des produits. – Tracking des produits sur le site. – Plannings d'acheminement.	– Risque de démarque. – Risque de casse et d'accident. – Retards d'expédition. – Dégradation des produits.	– Vérifier le correct acheminement vers les stocks. – Afficher les itinéraires d'acheminement pour chaque type de références sur les sites de sortie de chaîne. – Prendre en considération la nature des produits lors de l'acquisition du matériel de manutention. – Etablir des plannings d'acheminement en collaboration avec le service de gestion des stocks.
	– Être sûr que les produits retournés sont pris en compte par le service (recyclage...) et traités.	– Manque de communication avec le service SAV.	– Bon de retour des produits. – Fiche d'anomalie du produit retourné.	– Produits retournés non traités. – Problème de stockage à cause de la multitude de produits non traités.	– Travailler en collaboration avec le service SAV. – Etablir une fiche d'anomalies types pour chaque produit.

PROCESSUS ET/OU DOMAINE DE GESTION : production et services connexes					
Étapes/Sous-domaines	FINALITÉS (objectifs de contrôle interne)	RISQUES			EXEMPLES de bonnes pratiques de contrôle interne
		Facteurs (scénarios d'empêchement)	Points de contrôle	Impacts	
Activités de contrôle (découpage du processus et/ou domaine de gestion)					
7. Veille technologique	– Être sûr que les machines existantes sont aptes à intégrer les nouvelles technologies.	– Parc industriel vieillissant et non adaptable. – Utilisation de technologies en fin de vie. – Outil de production surspécialisé compte tenu des exigences de l'activité.	– Liste des contraintes techniques. – Plan de fabrication. – Contraintes techniques.	– Non-atteinte des objectifs. – Risque de perte de qualité. – Difficulté d'effectuer une maintenance correcte entraînant obligation de rachat.	– Élaborer une liste exhaustive des contraintes techniques de fabrication et la mettre à jour systématiquement.
	– Être sûr que les usines et la direction technique s'informent constamment des dernières avancées technologiques qui peuvent avoir un impact négatif ou positif sur l'organisation.	– La direction n'a pas accès aux informations relatives aux dernières avancées technologiques. – Non-prise en compte par la direction d'informations pertinentes qui pourraient s'avérer utiles dans le cadre d'un projet de développement autre que ceux auxquels les personnes des services développement sont associées.	– Notes de synthèse des progrès technologiques. – Procédure de diffusion d'information et de recueil des besoins et opportunités.	– Perte de compétitivité de la société par rapport à ses concurrents. – Non-optimisation de l'activité de la société.	– Suivi des documents publiés sur l'environnement économique, la technique et l'industrie dans lesquels évolue l'organisation. – Participation à des séminaires, conférences, salons, expositions... – Notes de synthèse des progrès technologiques observés ou réalisés y compris des projets de recherche en cours prévus. – Diffusion des notes de synthèse aux niveaux appropriés. – Existence d'un circuit d'information et de recueil des besoins et opportunités par activité.

 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration
 Illustration

 Illustration

 Illustration

L'Essentiel

- Les référentiels de risques constituent un véritable cadre de référence dans le déroulement d'une mission d'audit.
- Qu'ils soient établis en phase de préparation d'une nouvelle thématique à auditer ou répertoriés dans une bibliothèque de référentiels existants, ils représentent une garantie quant à l'exhaustivité des différents thèmes à auditer, au degré de détail approprié des investigations à mener ou encore à l'achèvement de la mission dans les délais prévus.

Chapitre 11

Illustrations et cas pratiques

EXECUTIVE SUMMARY

- Nous proposons un quiz et une grille d'autodiagnostic de la méthodologie présentée dans ce livre en rapport avec celle appliquée au sein de votre organisation afin d'y noter les convergences et différences et chercher des pistes de réflexion et/ou d'amélioration.
- Le référentiel COSO 2013, dit COSO « contrôle interne », est composé de cinq composantes et décliné en dix-sept principes. Nous avons souhaité, pour chacun de ces principes, donner des illustrations montrant comment les entreprises nationales ou internationales communiquent à ce niveau sur leur site Internet.
- Enfin, nous présentons en fin d'ouvrage une étude de cas permettant de s'entraîner à identifier des risques, produire des FAR (fiches d'audit et de recommandations) et visualiser un rapport d'audit.

QUIZ

Révision des connaissances – Énoncé

Vous souhaitez évaluer vos connaissances à l'issue de la lecture de cette nouvelle édition de l'ouvrage ? Nous vous proposons une série de questions puis un corrigé type. Pour mémoire, des vidéos de synthèse de la méthodologie d'audit sont disponibles sur le site Internet suivant : <http://www.audit-interne-referentiels-risques.fr>.

Définition de l'audit interne

La définition française de l'audit interne (IFACI) remonte au 21 mars 2000.

En relisant cette définition, quels sont les mots clés qui vous viennent à l'esprit lorsqu'on parle d'audit interne ?

Le concept de risque

Il est indiqué dans l'ouvrage que le « risque » est un concept signifiant la possibilité que la combinaison d'un événement et d'un mode de fonctionnement inapproprié empêche l'atteinte d'un objectif.

En regard des trois constituants d'un risque évoqués ci-dessus, quelles sont les mesures palliatives qui constituent des éléments du dispositif de contrôle interne à mettre en place ?

Le contrôle interne

Le référentiel COSO I (1992) se présentant sous forme d'une pyramide a été actualisé en 2013 sous la forme d'un cube, avec l'appellation de COSO « contrôle interne ». Il est composé de cinq composantes et décliné en dix-sept principes complétés par des points d'attention et des illustrations.

Quels sont les cinq composantes du référentiel et les dix-sept principes attachés ?

Évaluez votre méthodologie d'audit

Notez les convergences et différences entre les méthodologies d'audit interne employées dans les entreprises que vous connaissez et celle proposée dans cet ouvrage.

Étapes	Convergences	Différences constatées	Causes	Avantages	Inconvénients
1. Le droit d'accès : la lettre ou l'ordre de mission					
2. L'examen de l'activité et son découpage en objets auditables					
3. Le référentiel d'audit : l'élaboration d'un tableau des risques					
4. La réunion d'ouverture ou d'installation de l'équipe					
5. L'analyse des forces et faiblesses apparentes					
6. Le rapport d'orientation ou la note de cadrage					
7. Le programme de vérifications					
8. La formalisation des travaux de contrôle					
9. La fiche d'audit et de recommandations (FAR)					
10. L'ossature du rapport					
11. Le compte rendu oral sur site					
12. La rapport d'audit et sa validation					
13. Le suivi des recommandations					
14. L'état des actions de progrès.					

D'autres thèmes du quiz sont à retrouver en ligne :

www.audit-interne-referentiels-risques.fr.

Révision des connaissances – Corrigé

Définition de l'audit interne

- Activité
- Indépendante et objective/impartiale
- Valeur ajoutée
- Assurance et conseils
- Aide à atteindre objectifs
- Approche systématique et méthodique

- Évaluation et amélioration
- Processus de management des risques, de contrôle et de gouvernement d'entreprise

Le concept de risque

Constituants d'un risque	Mesures palliatives
Facteur ou cause organisationnelle	Prévention
Événement qui (peut) se manifeste(r)	Détection
Impact ou conséquence	Protection (dont assurance)

Le contrôle interne

Le référentiel COSO 2013 dit COSO « contrôle interne » est composé de cinq composantes et décliné en dix-sept principes. Vous trouverez plus bas, pour chacun de ces principes, des illustrations montrant comment les entreprises nationales ou internationales communiquent à ce niveau sur leur site Internet.

Tableau 11.1

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

ILLUSTRATIONS DES 17 PRINCIPES DU COSO

P1 L'organisation démontre son engagement en faveur de l'intégrité et des valeurs éthiques

Le groupe EDF promeut la culture d'intégrité et applique la tolérance zéro en matière de fraude et de corruption. Une conduite éthique et conforme aux lois est la règle absolue pour tous les salariés du groupe, à tous les niveaux de l'entreprise, sans exception.



& CHARTRE ÉTHIQUE GROUPE

« Nous nous devons
d'être exemplaires dans
nos comportements et
de promouvoir l'éthique dans
l'ensemble de nos activités
professionnelles. »

Jean-Bernard LEVY
Président-directeur général



Les valeurs du Groupe



Respect

Respecter les salariés en tant que personnes, leurs droits et fonder nos relations professionnelles au sein du Groupe sur l'écoute, le dialogue, la confiance et l'esprit d'équipe.

Bannir tout comportement de harcèlement ou de discrimination, prévenir et traiter dans la vie au travail toute situation de violence physique ou morale, d'intolérance ou d'injustice.

Respecter les opinions de chacun, y compris politiques, syndicales ou religieuses, à la condition que leur expression ne porte pas atteinte aux lois et règlements ; s'interdire de les imposer aux autres.

Protéger l'environnement en maîtrisant les risques, et être vigilant sur les impacts de nos activités vis-à-vis des personnes et de la nature.



Solidarité

- Agir pour le collectif, et favoriser la cohésion sociale au sein du Groupe.

- Accompagner les personnes les plus fragiles – parmi nos collègues ou les tiers, notamment les hommes et les femmes en situation de handicap ou nos clients en précarité énergétique.

- Favoriser l'accès au savoir ainsi que la transmission des connaissances – en particulier entre les générations de salariés du Groupe.

- Être un acteur engagé dans les situations d'urgence, en soutien aux populations, en France, en Europe et dans le reste du monde.



Responsabilité

- Garantir la sûreté de nos ouvrages et de nos installations industrielles, assurer la santé et la sécurité des personnes concernées par nos activités.

- Être à l'écoute et agir avec honnêteté, impartialité, équité et transparence à l'égard des salariés, clients, fournisseurs, partenaires, actionnaires, associations et pouvoirs publics.

- Pratiquer la tolérance zéro à l'égard de la fraude et de la corruption sous toutes leurs formes.

- Protéger le patrimoine matériel et immatériel, traiter de façon responsable les informations sensibles, et respecter les réglementations de protection des données personnelles.

Ces valeurs fondent notre identité et marquent notre fierté.
Elles confortent notre engagement d'assurer une relation de confiance auprès
de tous nos interlocuteurs. Elles sont le garant de la cohésion du Groupe.

Les documents de référence reposent sur trois textes normatifs que sont :

- la politique d'éthique et de conformité du groupe qui recense les programmes de conformité de l'entreprise ainsi que les

principales règles que les dirigeants doivent impérativement connaître, respecter et faire respecter dans leurs entités, en stricte adéquation avec les risques de ces entités ;

- la charte d'éthique du groupe construite autour des trois valeurs du groupe (respect, solidarité, responsabilité), qui place les exigences éthiques au cœur de la responsabilité de l'entreprise et promeut les comportements éthiques au sein du collectif de travail ;
- le « code de conduite », document de référence en matière de prévention de la corruption qui s'applique à tous les salariés du groupe et constitue un des piliers du programme de conformité relatif à l'application de la loi Sapin 2.

Figures 11.2 et 11.3



CODE DE CONDUITE ÉTHIQUE ET CONFORMITÉ

LES 9 RÈGLES D'OR



« J'ai voulu que notre Code de conduite soit de portée large et décrive différentes formes de corruption possibles, afin de nous protéger de la manière la plus efficace qui soit et de sauvegarder l'excellente réputation de notre Groupe. »

Jean-Bernard Lévy, président-directeur général d'EDF



Prévention de la corruption

Ne participons pas et n'autorisons jamais un acte de corruption. Aucun salarié ne sera sanctionné s'il respecte les règles d'EDF en refusant toute forme de corruption, même si une telle décision peut entraîner la perte d'un contrat ou toute autre conséquence commerciale défavorable.



Contrôle d'intégrité des relations d'affaires

La réputation d'EDF pouvant être affectée de manière significative par ceux que nous choisissons dans le cadre de nos relations d'affaires, il est impératif de ne traiter qu'avec des partenaires qui respectent les règles d'intégrité et les valeurs du groupe EDF.



Cadeaux et invitations

En matière de cadeaux et invitations, le plus important est d'agir en toute transparence vis-à-vis de notre hiérarchie, de rester dans les limites du raisonnable et de toujours nous interroger sur la façon dont cela pourrait être perçu ou interprété par un regard extérieur.



Prévention des conflits d'intérêts

Communiquons à notre hiérarchie tout conflit d'intérêts potentiel, le plus en amont possible de la relation, et prenons toujours, dans le cadre professionnel, des décisions en fonction des intérêts d'EDF, et jamais en fonction de notre intérêt personnel.



Lutte contre la fraude

Respectons les lois et les procédures internes, contribuons à la mise en place de pratiques rigoureuses et appliquons-les, détectons et traitons les dysfonctionnements.



Prévention des abus de marché

N'utilisons pas et ne divulguons jamais d'informations privilégiées ou sensibles, afin d'en tirer un bénéfice personnel ou de permettre à un tiers d'en tirer profit.



Prévention du risque de blanchiment de capitaux et de financement du terrorisme

Il est impératif de bien connaître nos relations d'affaires, notamment le bénéficiaire final de nos financements ou services, afin de nous assurer que nos activités ne servent pas à « blanchir » des fonds en provenance d'activités criminelles, ou à financer directement ou indirectement des activités liées au terrorisme.



Prévention des manquements au droit de la concurrence

Ne partageons pas avec nos concurrents des informations portant sur des sujets tels que les prix, les coûts ou la stratégie, car cela pourrait engendrer des soupçons de manipulation ou de distorsion de concurrence. Ne concluons jamais d'accord avec des concurrents dans le but de fausser la libre concurrence sur un marché.



Respect des sanctions internationales et contrôle des échanges internationaux

Vérifions, préalablement à tout engagement, que notre relation d'affaires ne figure sur aucune liste de sanctions internationales et soyons toujours au courant de ce que nous exportons, de sa destination, de son utilisateur final et de son utilisation réelle.

P2 Le conseil d'administration fait preuve d'indépendance vis-à-vis du management et surveille la mise en place et le bon fonctionnement du système de contrôle interne

« Un administrateur est indépendant lorsqu'il n'entretient aucune relation de quelque nature que ce soit avec la société, son groupe ou sa direction, qui puisse compromettre l'exercice de sa liberté de jugement. Ainsi, par administrateur indépendant, il faut entendre non pas seulement administrateur non-exécutif, c'est-à-dire n'exerçant pas de fonctions de direction de la société ou de son groupe, mais encore dépourvu de liens d'intérêt particulier (actionnaire significatif, salarié, autre) avec ceux-ci.

Pour une bonne pratique de gouvernement d'entreprise, le conseil procède à l'évaluation de sa capacité à répondre aux attentes des actionnaires qui lui ont donné mandat d'administrer la société, en passant en revue périodiquement sa composition, son organisation et son fonctionnement (ce qui implique une même revue des comités du conseil).

La loi a consacré le principe selon lequel le président ou le directeur général est tenu de communiquer à chaque administrateur tous les documents et informations nécessaires à l'accomplissement de sa mission. Les modalités d'exercice de ce droit de communication et les obligations de confidentialité qui lui sont attachées doivent être précisées par le règlement intérieur du conseil d'administration auquel revient, le cas échéant, le soin d'apprécier le caractère utile des documents demandés.

L'une des conditions majeures de la nomination d'un administrateur est sa compétence, mais il ne peut être attendu *a priori* de tout administrateur une connaissance précise de l'organisation de l'entreprise et de ses activités. Chaque administrateur doit donc bénéficier, s'il le juge nécessaire, d'une formation complémentaire sur les spécificités de l'entreprise, ses métiers et son secteur d'activité. » Code AFEP MEDEF.

Voici l'exemple d'Orange : document d'enregistrement universel 2019.

Figure 11.4

Orange se réfère au code Afep-Medef de gouvernement d'entreprise des sociétés cotées révisé en janvier 2020, consultable sur les sites Internet d'Orange, de l'Afep et du Medef.

En application de la règle *Appliquer ou Expliquer* (« comply or explain ») prévue à l'article L. 225-37 du Code de commerce, la Société déclare se conformer, à la date de ce document, aux recommandations du

code Afep-Medef à l'exception de la règle relative à la perte de la qualité d'administrateur indépendant (article 9.5.6 du Code Afep-Medef), laquelle intervient à la date des douze ans. Il est précisé que le mandat de Charles-Henri Filippi a atteint les douze années d'ancienneté le 5 février 2020 et que son mandat prend fin à l'issue de l'Assemblée générale du 19 mai prochain sans proposition de prolongation (voir section 5.2.1.2 *Administrateurs indépendants*).

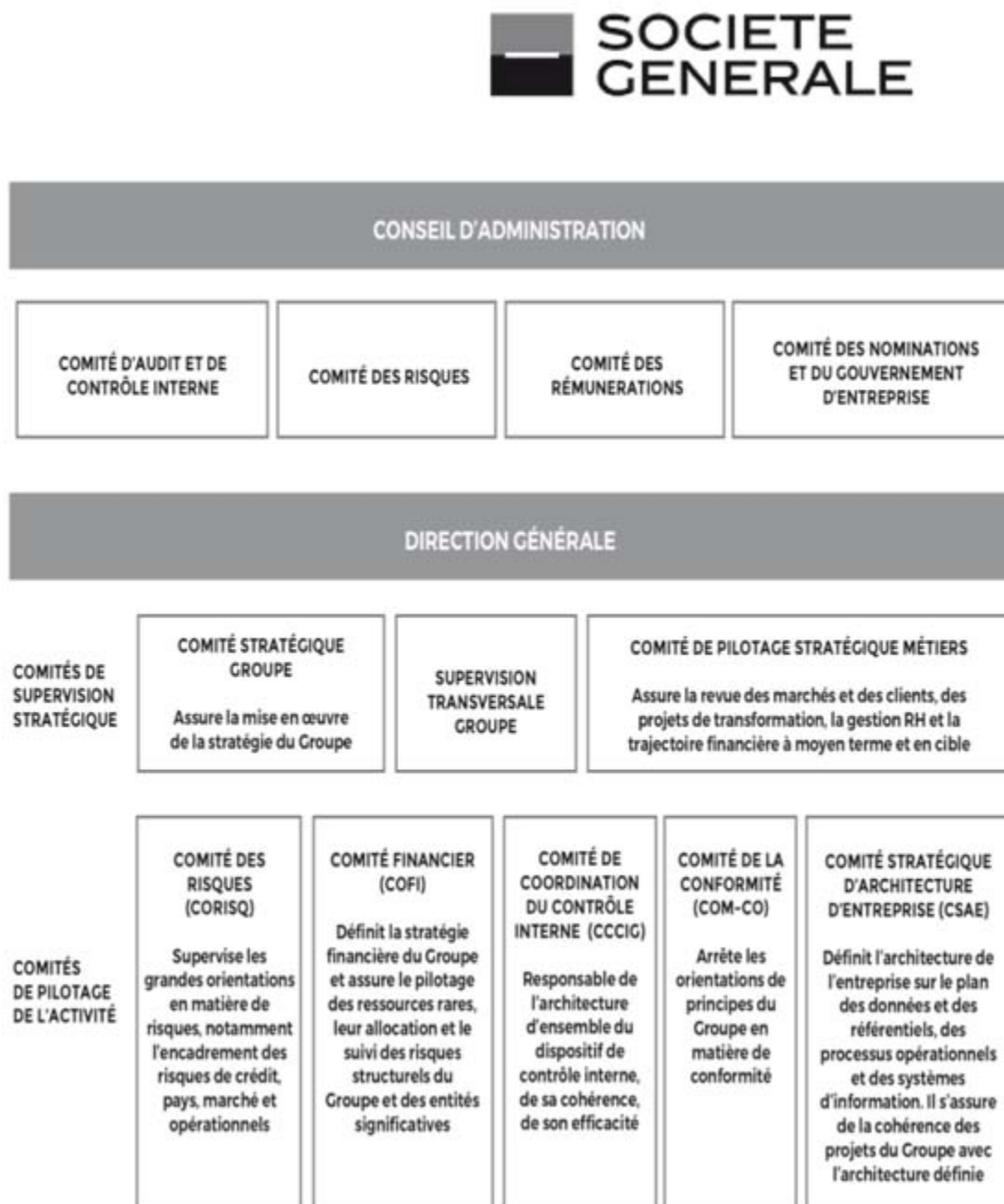
Principales différences avec les règles du New York Stock Exchange

Orange s'attache à prendre en compte les règles du New York Stock Exchange (NYSE) en matière de gouvernement d'entreprise. Toutefois, parce que la Société n'est pas américaine, la plupart de celles-ci ne s'imposent pas à elle, la Société étant autorisée à suivre à leur place les règles applicables en France. C'est ainsi qu'Orange a choisi de se référer au code Afep-Medef dont les recommandations diffèrent, sur certains points, des règles applicables aux sociétés américaines cotées sur le NYSE.

Les principales différences entre les pratiques d'Orange et les règles applicables aux sociétés américaines sont décrites dans le rapport annuel d'Orange (*Form 20-F*) enregistré auprès de la *Securities and Exchange Commission* des États-Unis.

P3 La direction, agissant sous la surveillance du conseil d'administration, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour atteindre les objectifs

Figure 11.5



P4 L'organisation démontre son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs

Figure 11.6



BÉNÉFICIEZ DE **CONDITIONS MOTIVANTES**
CONTRIBUEZ À UN **AVENIR ÉNERGÉTIQUE RESPONSABLE**

DÉVELOPPEZ VOTRE **POTENTIEL DE COMPÉTENCES**

DÉCOUVREZ D'ÉTONNANTES **POSSIBILITÉS DE PARCOURS**

RELEVEZ DE **PASSIONNANTS DÉFIS**



P5 L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne

Objectif chez LVMH : vérifier si le devoir de chacun de rendre compte de ses responsabilités en matière de contrôle interne est bien respecté.

- Rapport du président du CA sur le contrôle interne.
- Le groupe explique que son référentiel est établi en cohérence avec le référentiel COSO.
- Mise en évidence dans les composantes du contrôle interne d'« un système d'information et de communication permettant l'exercice

efficace des responsabilités ».

- Afin de communiquer en interne, LVMH a mis en place un intranet utilisé pour de multiples informations. L'une d'entre elles consiste en la diffusion des principes et bonnes pratiques de contrôle interne.
-

Figure 11.7



2.3 Les composantes du contrôle interne

Le dispositif de contrôle interne, suivant l'approche COSO qui a été retenue, comprend cinq composantes étroitement liées :

- un environnement général de contrôle ;
- une évaluation des risques ;
- des contrôles appropriés ;
- un système d'information et de communication permettant l'exercice efficace des responsabilités ;
- un plan de suivi et de progrès.

Tous ces éléments sont à la fois pilotés et coordonnés centralement et examinés annuellement par les entités significatives du Groupe par le biais de la démarche d'auto-évaluation en place.

P6 L'organisation spécifie les objectifs de façon suffisamment claire pour permettre l'identification et l'évaluation des risques associés aux objectifs

Figure 11.8



Stratégie et objectifs

Poursuivant sa success story, Volkswagen Group se transforme pour devenir le leader de la mobilité durable. Un nouveau chapitre qui amène à faire évoluer l'activité de pur constructeur de véhicules vers celle de fournisseur de mobilité :

- Ce tournant va connecter de plus en plus l'automobile au monde digital et a donné naissance à MOIA, la nouvelle société de services de mobilité du Groupe.
- La nouvelle offre du Groupe s'enrichira de plus de 30 nouveaux modèles électriques d'ici 2025 cohabitant avec l'optimisation constante des moteurs essence ou diesel.
- Le design sera plus que jamais un facteur clé de l'expérience utilisateur et de l'attachement à la marque.

UNE NOUVELLE VISION

Pour devenir le premier fournisseur de mobilité durable

4 piliers de la croissance responsable :

1. Servir des clients heureux
2. Être reconnu comme un excellent employeur
3. Maintenir une rentabilité compétitive
4. Devenir une référence pour l'environnement, la sécurité et l'intégrité

4 MISSIONS ESSENTIELLES

Pour mettre la confiance au cœur de notre avenir

Elles sont d'ores et déjà centrales dans l'action quotidienne des collaborateurs et au cœur des décisions stratégiques :

- TRANSFORMER notre cœur de métier
- RENFORCER notre pouvoir d'innovation
- SÉCURISER nos investissements
- AGIR avec intégrité

3 INITIATIVES

Pour réussir une transformation historique

DIGITALISATION

Initiative majeure du Groupe, cette orientation concerne le passage au Business 4.0 et le déploiement de laboratoires du futur du digital. Signe fort : le Chief Digital Officer, poste nouvellement créé et occupé par Johann Jungwirth (ex-Apple/Mercedes), dépend directement de la présidence du Groupe.

CROISSANCE RESPONSABLE

C'est la clé pour occuper la place de leader de la mobilité du futur, inscrite dans le développement durable.

- Un projet global majeur autour de l'électromobilité :
 - 30 nouveaux véhicules électriques d'ici 2025,
 - 2 à 3 millions d'unités vendues par an en 2025,
 - 20 à 25 % des ventes unitaires attendues pour cette période.
- Le développement de la technologie des batteries électriques (autonomie, temps de charge, recyclage...) comme nouvelle compétence générant des revenus associés.
- L'investissement dans les offres de mobilité à la demande (VTC, taxis robots, covoiturage...).
- Le développement de moteurs conformes et innovants sur les autres énergies.

CONFORMITÉ / INTÉGRITÉ

La nouvelle stratégie du Groupe a placé l'intégrité au cœur de son ADN, en créant notamment une nouvelle fonction au sein du comité de direction. Ces notions vont donc s'ancrer durablement au cœur des process et des décisions quotidiennes pour enclencher un cercle vertueux en termes de réputation comme en termes de résultats opérationnels.

P7 L'organisation identifie les risques associés à la réalisation de ses objectifs dans l'ensemble de son périmètre de responsabilité et elle procède à leur analyse de façon à déterminer les modalités de gestion des risques appropriées

Figure 11.9



La gestion des risques du Groupe s'articule autour des principales catégories suivantes :

- **Le risque de crédit et de contrepartie** : risque de pertes résultant de l'incapacité des clients du Groupe, d'émetteurs ou d'autres contreparties à faire face à leurs engagements financiers. Le risque de crédit inclut le risque de contrepartie afférent aux opérations de marché, le risque lié aux activités de titrisation et peut être aggravé par le risque de concentration individuelle, pays ou sectorielle ;
 - **Le risque de marché** : risque de pertes de valeur d'instruments financiers, résultant des variations de paramètres de marché, de leur volatilité et des corrélations entre ces derniers. Les paramètres concernés sont notamment les taux de change, les taux d'intérêt, les prix des titres (actions, obligations) et des matières premières, des dérivés et de tout autre actif ;
 - **Les risques opérationnels** : risque de pertes résultant d'une défaillance des processus, du personnel et des systèmes d'information ou d'événements extérieurs. Cette catégorie de risque comprend notamment :
 - les **risques de non-conformité** (y compris les **risques juridiques et fiscaux**) : risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative ou d'atteinte à la réputation, qui naît du non-respect des dispositions propres aux activités bancaires et financières qu'elles soient de nature législative ou réglementaire, nationales ou européennes directement applicables, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions des dirigeants effectifs prises notamment en application des orientations de l'organe de surveillance,
 - le **risque de réputation** : risque résultant d'une perception négative de la part des clients, des contreparties, des actionnaires, des investisseurs ou des régulateurs, pouvant affecter défavorablement la capacité du Groupe à maintenir ou engager des relations d'affaires et la continuité d'accès aux sources de financement,
 - le **risque de conduite inappropriée « misconduct »** : risque résultant d'action (ou d'inactions), ou de comportements de la Banque, ou de ses employés, qui seraient incompatibles avec le Code de conduite du Groupe, pouvant aboutir à des conséquences négatives pour nos parties prenantes, ou mettant en risque la pérennité ou la réputation de la Banque,
 - les **risques IT et de la Sécurité des Systèmes d'information** (cybercriminalité, défaillance de services...);
 - **Le risque de modèle** : risque de conséquences adverses de décisions fondées sur des résultats et des rapports de modèle incorrects ou mal utilisés ;
 - **Les risques structurels** : risques de pertes de marge d'intérêt ou de valeur du portefeuille bancaire en cas de variation des taux d'intérêt et de change. Ce risque est lié aux activités commerciales et aux opérations de gestion propre et inclut le risque de déformation de l'écart structurel entre les actifs et les passifs liés aux engagements sociaux ainsi que le risque associé au rallongement de durée de versements futurs ;
 - **Le risque de liquidité et de financement** : le risque de liquidité se définit comme l'incapacité pour le Groupe à faire face aux échéances de ses obligations financières à un coût raisonnable. Le risque de financement se définit comme le risque pour le Groupe de ne pas pouvoir financer le développement de ses activités selon ses objectifs commerciaux et à un coût compétitif par rapport à ses concurrents ;
 - **Le risque stratégique/business** : risque résultant de l'incapacité du Groupe à mettre en œuvre sa stratégie et à réaliser son business plan pour des raisons ne relevant pas des autres risques de cette nomenclature; par exemple la non-réalisation de scénarios macroéconomiques ayant servi à construire le business plan ou une performance commerciale moindre qu'escomptée ;
 - **Le risque de baisse de la valeur des participations en capital dans certaines sociétés** : baisse de la valeur de nos participations en actions ;
 - **Le risque lié aux activités d'assurance** : risque de pertes inhérent à l'activité d'assureur auquel le Groupe est exposé à travers ses filiales d'assurance. Il s'agit, au-delà de la gestion des risques actif-passif (risques de taux, de valorisation, de contrepartie et de change), du risque de tarification des primes, du risque de mortalité et d'augmentation de la sinistralité ;
 - **Le risque de valeur résiduelle** : au travers de ses financements spécialisés, principalement sa filiale de location longue durée de véhicules, le Groupe est exposé au risque de valeur résiduelle (valeur nette de revente d'un actif à la fin du contrat de crédit-bail ou de location inférieure à l'estimation).
- Par ailleurs, les **risques liés aux changements climatiques** qu'ils soient de type physique (augmentation de fréquence d'occurrence d'événements climatiques extrêmes) ou de transition (nouvelles réglementations carbone) sont identifiés comme des facteurs aggravants des autres risques existants.

P8 L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles de compromettre la réalisation des objectifs

Figure 11.10



Chez Schneider Electric, un comité des fraudes définit la politique de lutte contre la fraude ainsi que le processus de déclaration et de traitement des fraudes et soupçons de fraude. Il est composé du directeur juridique et responsable de la conformité, du directeur de la sûreté mondiale et du directeur de l'audit interne et des contrôles internes ; il se réunit à une fréquence mensuelle et selon les besoins. Il traite également les cas de fraude, de corruption, de conflit d'intérêts, de violation de procédure, de vol et les cas connexes.

Les investigations sont décidées par le comité des fraudes et pilotées en fonction de l'importance du sujet et du niveau hiérarchique potentiellement impliqué. Le comité s'assure également de la mise en place du plan d'actions, de la sanction appropriée ainsi que du retour d'expérience pour chaque fraude avérée. Un reporting est établi et mis à jour régulièrement à cet effet. Une synthèse annuelle est présentée au comité d'audit.

La direction de la sûreté est également directement impliquée dans la lutte contre la fraude interne (pilotage et réalisation d'investigations internes). Elle s'est dotée en 2013 d'un « bureau des recherches de Schneider Electric », chargé de la conduite des investigations (fraudes internes et externes) qui apporte son soutien aux investigateurs internes. Elle définit par ailleurs les méthodologies et procédures à suivre pour mener à bien les investigations, dans le respect de la loi et aux fins de réunir efficacement des preuves.

P9 L'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle interne

Les dispositifs de protections des données d'Amazon ont été modifiés suite à la promulgation du Règlement général sur la protection des données (RGPD).

Figure 11.11



Tous les services AWS sont prêts pour le RGPD – En savoir plus

Outre notre propre conformité, AWS s'engage à offrir des services et des ressources à nos clients pour leur permettre de respecter les exigences du RGPD susceptibles de s'appliquer à leurs activités. De nouvelles fonctions sont lancées régulièrement et AWS propose **plus de 500 fonctions et services** axés sur la sécurité et la conformité.

Podcast : Respect du RGPD avec AWS Key Management Service (KMS)

Tableau : Capacités de service AWS pour le RGPD

Blog : RGPD DPA d'AWS – Désormais partie intégrante des Conditions d'utilisation

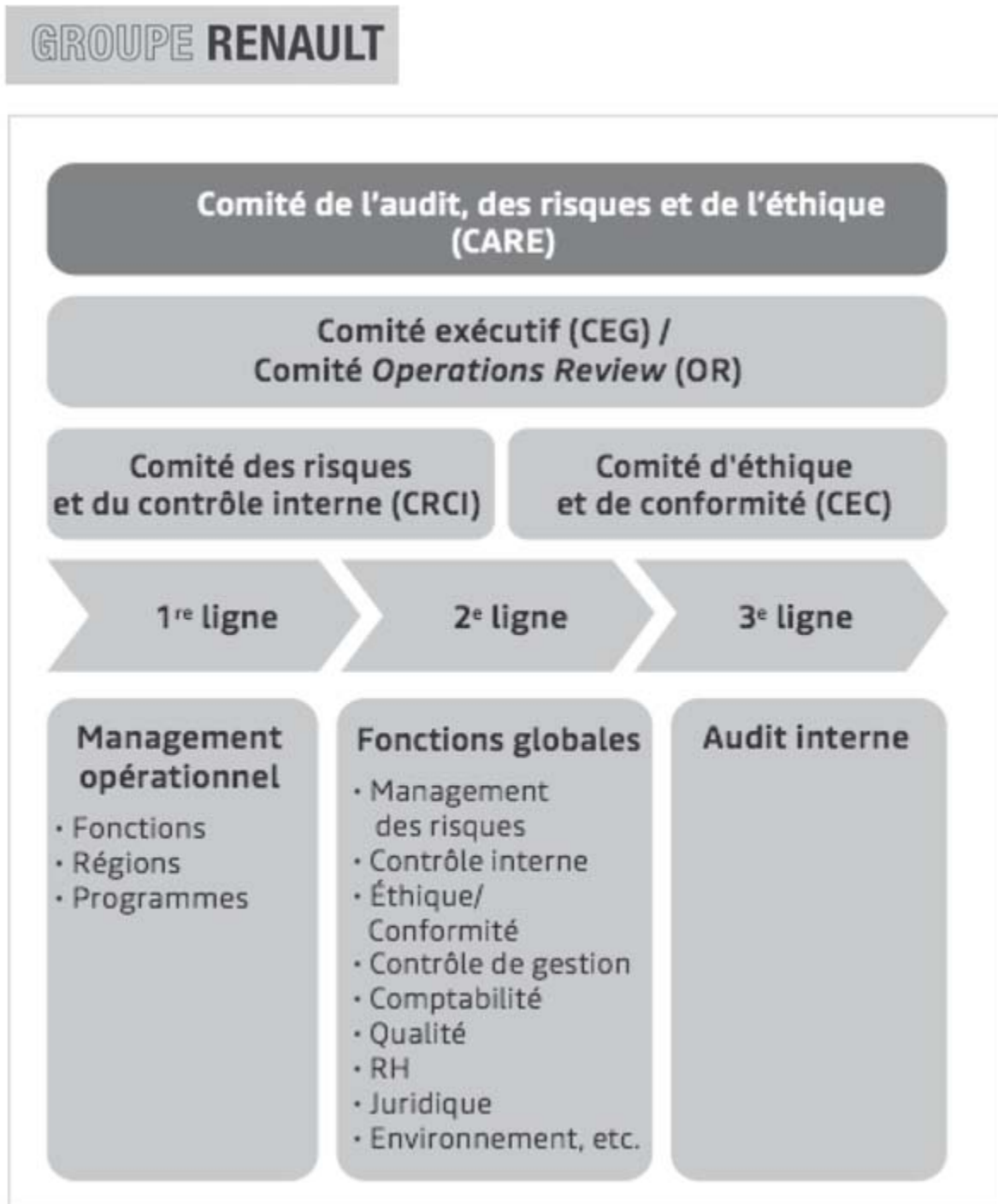
Blog : Soutien des clients AWS et des partenaires APN en quête de conformité avec le RGPD

Blog : Modèle de responsabilité partagée d'AWS et RGPD

P10 L'organisation sélectionne et développe les activités de contrôle qui contribuent à ramener à des niveaux acceptables les risques associés à la réalisation des objectifs

Le groupe Renault organise ses activités de contrôle regroupées dans le CARE. Ces dernières sont réparties en trois niveaux allant des opérationnels au service d'audit interne.

Figure 11.12



P11 L'organisation sélectionne et développe des activités de contrôle général en matière de système d'information

pour faciliter la réalisation des objectifs

La direction des systèmes d'information du groupe Lagardère met en place des contrôles conçus pour :

- identifier et minimiser les risques (intrusions, interruption des services) ;
- participer à l'actualisation de l'organisation et de la sécurité générale des SI ;
- aider au développement de son réseau de communication à l'international.

Ces informations sont tirées du chapitre 7 du document de référence 2018, « Informations concernant l'organisation de la Société et du Groupe ».

Figure 11.13

Lagardère

SÉCURITÉ DES SYSTÈMES ET RÉSEAUX INFORMATIQUES

La Direction des Systèmes d'Information effectue de manière récurrente avec la Direction des Risques des enquêtes d'auto-évaluation de la sécurité des systèmes et réseaux informatiques. Les domaines traités sont :

- l'organisation et la sécurité générale des systèmes d'information ;
- la sécurité physique (intrusion, accidents) ;
- les postes de travail (administration et protection) ;
- les réseaux (locaux, distants, internet) ;
- les contrôles d'accès aux ressources ;
- la disponibilité des applications et des données.

Les résultats de ces enquêtes permettent d'actualiser l'ensemble des mesures visant à préserver la confidentialité des données, protéger les systèmes informatiques contre les intrusions et minimiser les risques d'interruption de service de ces mêmes systèmes.

Par ailleurs une charte d'utilisation des systèmes informatiques s'impose à l'ensemble des salariés du Groupe.

Enfin, le Groupe poursuit le déploiement de son réseau de communication sécurisé, en France et à l'international.

P12 L'organisation met en place les activités de contrôle par le biais de directives qui précisent les objectifs poursuivis et de procédures qui mettent en œuvre ces directives

Safran a mis en place un référentiel de procédures pour s'assurer de la qualité et de la fiabilité des informations utilisées.

Figure 11.14



D) ACTIVITÉS ET FONCTIONNEMENT DE LA GESTION DES RISQUES ET DU CONTRÔLE INTERNE

1) Les activités du contrôle interne

a) Le référentiel des procédures

Les principales procédures intéressant le fonctionnement du Groupe sont rassemblées dans un système documentaire accessible via l'intranet du Groupe et comprenant notamment :

- les règles comptables IFRS Groupe ;
- les règles d'élaboration des comptes consolidés et celles relatives aux opérations intra-groupe ou inter-compagnies ;
- les instructions trimestrielles relatives à la consolidation diffusées à l'ensemble des sociétés concernées ;
- le guide d'utilisation du progiciel de consolidation ; ce progiciel contenant les contrôles nécessaires à la cohérence des divers éléments constituant la consolidation des comptes ;
- les règles et procédures d'utilisation de l'ERP Groupe (Movex/M3) ;
- les procédures de suivi spécifique des encours de crédit des compagnies aériennes ;
- les procédures de gestion et de suivi du risque de change ;
- les procédures liées aux formats et contenus "standards Groupe" de reporting et budget ;
- les procédures liées aux contrôles Qualité, accidents du travail, etc.

Le Groupe a initié en juin 2012 un projet d'amélioration du référentiel de procédure sur son intranet. Ce projet, avec une équipe internationale, a pour ambition d'améliorer la recherche d'informations via une navigation en ligne par processus clés.

b) Procédures budgétaires

La direction générale du Groupe définit les hypothèses économiques et financières générales conformément à la stratégie du Groupe.

Sur la base de ces orientations générales, les différentes branches préparent un projet de budget annuel, associé à l'élaboration d'un *business plan* pluriannuel. Cet ensemble est ensuite présenté à la direction générale du Groupe. Cette phase du processus permet d'acter les options opérationnelles à suivre par les branches et leurs divisions, ainsi que les évolutions à moyen et long terme au travers du *business plan*.

L'ensemble de ces budgets est également déposé dans une base de données Groupe accessible par les différents responsables concernés (société, division, branche, Groupe) à tous les stades du processus budgétaire.

P13 L'organisation obtient ou génère puis utilise des informations pertinentes et de qualité pour faciliter le fonctionnement des autres composantes du contrôle interne

PSA Groupe a mis en place un système de reporting RSE segmenté par secteur d'activité permettant d'avoir des informations organisées et pertinentes.

Figure 11.15



ACTIVITÉS INCLUSES DANS LE REPORTING ET ÉVOLUTIONS

Le périmètre sur lequel sont rapportées de façon détaillée les informations sociales, environnementales et sociétales sur les actions en faveur du développement durable inclut :

■ Les activités automobiles :

Ce périmètre regroupe les filiales PSA Automobiles SA et Opel Automobile GmbH (manufacturing facilities, R&D facilities and office sites) as well as commercial subsidiaries of the brands.

Sauf mention contraire, la politique du Groupe s'applique à PSA Automobiles SA. C'est le cas en particulier pour les thèmes suivants : conditions de santé et de sécurité au travail, organisation du dialogue social, notamment les procédures d'information et de consultation du personnel et de négociation, ainsi que les accords signés avec les organisations syndicales ou les représentants du personnel, les politiques mises en œuvre en matière de formation, la politique de lutte contre les discriminations, les actions menées en lien avec l'impact territorial du Groupe, les actions de partenariat ou de mécénat, la prise en compte dans la politique d'achat des enjeux sociaux et environnementaux.

La structure PCMA Automotiv RUS, située à Kaluga en Russie, en joint-venture avec Mitsubishi Motors Corp. est aussi incluse dans le périmètre de reporting, sur les volets sociétaux et environnementaux, car le Groupe en détient 70 % des parts ;

■ Les activités du commerce automobile :

Elles regroupent les sites du réseau commercial détenu en propre, les centres de formations pour les personnels du réseau, les magasins de pièces de rechange, les directions régionales et les sièges des filiales d'importation.

Le périmètre « activités du commerce automobile » est inclus dans l'appellation « division Automobile » pour les thématiques RH, mais il est traité à part pour les thématiques Environnement ;

■ Division Automobile :

La division Automobile rassemble les activités automobiles et les activités du commerce automobile.

Pour obtenir des informations RSE plus détaillées au sujet de la division Automobile, reportez-vous au rapport RSE ;

NOTA : pour les périmètres mentionnés ci-dessus, le présent reporting isole les données relatives à Peugeot, Citroën et DS (désignées « PCD », correspondant au périmètre historique, avant l'acquisition des sociétés Opel et Vauxhall par le Groupe PSA) et les données relatives à Opel et Vauxhall (désignées « OV »).

■ La filiale d'équipement :

Faurecia, société cotée dont le capital est détenu désormais à 46,3 % par le Groupe PSA reste consolidée par intégration globale car Peugeot S.A. conserve le contrôle (63,1 % des droits de vote théorique). Conformément aux dispositions légales, Faurecia dispose d'une complète autonomie de gestion qui établit et publie dans son propre document de référence les indicateurs sociaux, environnementaux et sociétaux relevant de son activité ;

■ Les autres activités :

Elles sont désormais composées de la société holding Peugeot S.A., et de Banque PSA Finance (BPF).

Concernant BPF, les informations sociales et sociétales publiées dans le document de référence consolident les entités détenues à 100 % par BPF au 31 décembre 2018. Cette méthodologie, alignée sur les règles de consolidation de BPF, exclut du périmètre de reporting RSE les joint-ventures créées avec Santander, dont la liste est présentée dans le rapport de gestion de BPF.

Conformément aux exigences réglementaires, les informations quantitatives ont été publiées sur la base d'indicateurs transversaux et consolidables, dès lors que ces informations étaient pertinentes.

P14 L'organisation communique en interne les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne, notamment

en ce qui concerne les objectifs et les responsabilités associés au contrôle interne

Carrefour Connect est l'intranet du groupe Carrefour. Cette plateforme interne collaborative connecte près de 400 000 collaborateurs à travers le monde avec la volonté de les faire participer au quotidien à l'actualité du groupe.

Les collaborateurs ont accès :

- aux actualités du groupe mais également du pays et du métier qui les concernent ;
- aux informations RH qui les concernent ;
- aux outils collaboratifs ;
- aux applications professionnelles utilisées au quotidien.

<https://vimeo.com/250113533>

Figure 11.16



De son côté, la Banque de France a mis en place un système d'intra-messagerie instantané permettant à l'ensemble de ses agents de communiquer et de faire circuler l'information sur les dossiers de cotation des entreprises. Le but de ce dispositif est d'uniformiser l'information au niveau de l'ensemble des succursales de la France.

Figure 11.17



**P15 L'organisation communique avec les tiers au sujet
des facteurs qui affectent le bon fonctionnement des autres
composantes du contrôle interne**

Sur son site Internet, le groupe Atos met à disposition de ses partenaires externes une base riche en informations, communiqués, rapports et présentations financières.

Figure 11.18



P16 L'organisation sélectionne, met au point et réalise des évaluations continues et/ou ponctuelles afin de vérifier si les composantes du contrôle interne sont bien mises en place et fonctionnent

Chez Airbus, l'audit interne réalise des évaluations continues et ponctuelles (notamment annuelles).

Contrôle continu :

- procédures standardisées basées sur les exigences des référentiels appliquées systématiquement pour chaque audit ;
- recommandations sur la gestion de risque avec catégorisation systématique de chaque audit par rapport au processus couvert par l'ERM ;
- suivi des actions et de la clôture des actions d'audits précédents, y compris celles liées à la gestion des risques (suivi basé à son tour sur la carte de couverture de l'audit et plan d'audit élaborés par rapport au risque) ;
- cycle d'audit pluriannuel basé sur les risques (partie d'un processus de planification de l'audit) ;
- coopération avec les auditeurs externes et la deuxième ligne de défense (échange de rapports, briefings trimestriels).

Contrôle annuel :

- audits dédiés et cycle des années précédentes ;
- analyse de la base de données des risques ;
- évaluation de la contribution de la deuxième ligne de défense.

Figure 11.19



P17 L'organisation évalue et communique les faiblesses de contrôle interne en temps voulu aux responsables

des mesures correctrices, notamment à la direction générale et au conseil d'administration

Principales missions : formulation de proposition au conseil d'administration en rapport avec les dirigeants (recommandation, composition, nomination, rémunération, jetons de présence...).

Figure 11.20



Au sein d'AXA, le comité d'audit est chargé d'évaluer et d'améliorer la qualité du reporting et de l'efficacité du contrôle interne et le comité de rémunération veille aux bonnes pratiques de gouvernance et aux choix adaptés des dirigeants.

Figure 11.21

Comité d'Audit

- s'assurer de la qualité de la procédure de *reporting* financier ainsi que de l'intégrité des résultats publiés et des informations communiquées dans les états financiers ;
- s'assurer du caractère adéquat et de l'efficacité du cadre de contrôle interne ainsi que celui de la gestion des risques ;
- s'assurer de l'efficacité, la performance et l'indépendance des auditeurs internes du Groupe ;
- émettre des recommandations quant au processus de sélection des Commissaires aux comptes, suivre la réalisation par les Commissaires aux comptes de leur mission, s'assurer du respect des conditions de leur indépendance, suivre la répartition de leurs honoraires et émettre des recommandations au Conseil en cas de services autres que la certification des comptes rendus par les Commissaires aux comptes.

ÉTUDE DE CAS : SOCIÉTÉ H.A.¹

- Introduction aux faiblesses d'organisation et de contrôle interne
- Entraînement à l'application de la méthodologie d'audit interne
 - Analyse des risques apparents → Réflexion
 - Nature des risques → Forces/Faiblesses
 - Vérifications → Nature des dysfonctionnements

SOCIÉTÉ H.A.

La société H.A., au chiffre d'affaires de 200 millions d'euros, élabore et vend des produits destinés à l'industrie. Son siège social est situé à Paris. Elle possède trois usines en Île-de-France qui emploient chacune 200 personnes.

Le siège s'occupe de tous les aspects financiers et administratifs (gestion de la trésorerie, paie, comptabilité...).

Les directeurs d'usine sont responsables du suivi et de la planification de la production.

A. PHASE D'ÉTUDE

Les interviews menées pendant la phase d'étude nous ont permis de réunir les informations suivantes sur les différents cycles de la société H.A.

1) Approvisionnement des stocks de matières premières

Le réapprovisionnement des stocks est effectué au fur et à mesure de la réception des commandes clients envoyées par le siège. Il est décidé par les directeurs d'usine en fonction de leur stock disponible.

Afin de répondre rapidement à la demande, les commandes sont passées directement aux fournisseurs habituels. Un double est alors transmis au siège qui est ainsi informé des achats engagés par les usines.

Données chiffrées :

Évolution des achats (M€)													
Usine	J	F	M	A	M	J	J	A	S	O	N	D	Total
1	3,0	1,5	4,0	10,0	3,0	1,5	1,0	1,5	4,5	15,0	1,5	1,5	48,0
2	1,5	1,5	4,0	6,0	1,5	3,0	1,0	1,0	6,0	9,0	1,0	1,0	36,5
3	1,5	4,5	3,0	16,0	6,0	3,0	1,5	3,0	10,5	3,0	3,0	1,0	56
Total	6,0	7,5	11,0	32,0	10,5	7,5	3,5	5,5	21,0	27,0	5,5	3,5	140,5

 Illustration

2) Réception des matières premières

Les matières premières sont reçues dans les usines par les magasiniers qui les rangent directement en stock et enregistrent les mouvements sur les fiches de stock d'après les bons de livraison remis par les fournisseurs.

Les factures sont adressées par les fournisseurs au siège parisien. Elles y sont toutes systématiquement classées avec les bons de commande correspondants.

L'établissement des chèques de règlement des fournisseurs est effectué par un comptable du siège aux conditions indiquées sur la facture, après comparaison entre le double de la commande, reçu de l'usine et la facture (type, quantités et prix).

3) Signature du titre de paiement

Ces chèques ou les ordres de virement sont alors transmis au directeur général pour signature puis envoyés aux fournisseurs par le comptable.

4) Acquisitions d'immobilisations

Tout investissement fait l'objet d'une demande d'acquisition qui doit être approuvée par le directeur de l'usine. Après approbation, la commande est effectuée. Les services comptables du siège reçoivent alors une copie de la demande approuvée et un double de la commande. Ces documents sont transmis au trésorier du siège.

La facture du fournisseur parvient directement au service comptable du siège, qui enregistre l'immobilisation dans le journal et dans le registre des immobilisations. Le comptable rapproche ensuite la facture avec le bon de commande et avec la demande approuvée. Le directeur signe la traite après vérification de ces trois documents.

Travail à faire : sur la base des informations recueillies sur la société H.A., identifier les faiblesses de l'organisation et déterminer les risques de contrôle interne qui leurs sont liés.

B. PHASE DE VÉRIFICATION

Les faiblesses de contrôle interne relevées lors de la phase d'étude nous ont amenés à faire effectuer des tests.

Test a : (cf. A.1.)

Travail effectué :

Sélection de 10 fournisseurs par usine.

Comparaison des conditions de paiement accordées par les fournisseurs à la société H.A. avec celles du secteur.

Résultats :

Dans tous les cas, des conditions de paiement moins favorables sont accordées à la société H.A. par rapport à la moyenne du secteur.

Des conditions de paiement différentes sont accordées par le même fournisseur (société FOUR) aux usines 1 et 3.

Test b : (cf. A.2.)

Travail effectué :

Sélection de 30 factures reçues en janvier, février et mars, et rapprochement avec les bons de commande et les bons de réception correspondants.

Résultats :

10 factures ont été payées alors que la marchandise n'était pas encore reçue.

5 factures ont été payées alors que la marchandise reçue n'était pas conforme à la commande (quantité ou qualité).

Dans deux cas, le fournisseur refuse d'accorder un avoir.

Test c : (cf. A.3.)

Travail effectué :

Sélection de 30 décaissements de montants significatifs dans le journal de banque du mois de mai.

Retour aux pièces justificatives de ces décaissements (bons de commande, bons de réception et factures).

Résultats :

Les pièces justificatives n'ont pu être retrouvées pour cinq d'entre eux.

Une facture a été payée deux fois.

Test d : (cf. A.4.)

Travail effectué :

Analyse des dossiers d'investissements réalisés sur l'année.

Résultats :

Aucun appel d'offres formalisé n'a été effectué.

Aucune recherche de modes de financement appropriés n'a été entreprise.

Le paiement d'une immobilisation a été réalisé alors qu'elle n'a pas encore été livrée à l'usine.

Le paiement d'une immobilisation a été réalisé alors que des problèmes techniques sont rencontrés pour son installation.

Travail à faire : sur la base des informations recueillies durant la phase d'étude et des résultats des tests de contrôle interne, rédiger les fiches d'audit et de recommandations (FAR) correspondant aux anomalies décelées.

Fiche d'audit et de recommandations (FAR)

FAR N°...

Problème : *[Il résume le dysfonctionnement de façon synthétique, autonome et percutante.]*

Constats : *[Ce sont les anomalies constatées lors des tests ou relevées lors des interviews.]*

Constats : *[Ce sont les anomalies constatées lors des tests ou relevées lors des interviews.]*

Conséquences : *[Ce sont les risques supportés par la société ou les incidences constatées lors de la réalisation des tests.]*

Solution proposée : *[Elle doit être efficace (réponse au problème) et adressée (fonction chargée de sa mise en oeuvre).]*

Corrigé

X.Y.Z. Holding

NOTE INTERNE

Direction :

Date

Service :

Référence

Émetteur :

Veuillez trouver, ci-joint, notre rapport d'audit global de la Société H.A.

La mission d'audit a été effectuée par M. Ch. DEMISS, chef de mission, et Mmes A. TRICE et O. DITOSSI, auditeurs.

Selon le temps qu'il veut consacrer à ce rapport, le lecteur lira :

- le résumé : l'essentiel y est dit, sans démonstration, pour les lecteurs qui veulent en être informés sans avoir à régler les problèmes ;
- ou l'ensemble du rapport en commençant par le résumé qui donne les lignes directrices ; le rapport détaillé, qui couvre quelques points supplémentaires, fournit les éléments et les modes de réflexion que l'audit interne a utilisés et veut partager avec les audités et la Direction.

Les constats et recommandations développés dans ce rapport ont été validés lors d'une réunion effectuée le 10 mars 2020.

Je prie les destinataires des recommandations de bien vouloir m'adresser leurs plans d'actions pour le 31 mars 2020, sur le formulaire ci-joint, conformément au processus décrit au verso.

O. SCAR

Directeur de l'Audit Interne

DESTINATAIRES :

Copie :

IMPORTANT

Ce document est un rapport d'audit.

Il est recommandé de **ne pas étendre sa diffusion** au-delà de la liste prévue :

- il contient des informations confidentielles ;
- son style peut surprendre un lecteur non averti.

Un rapport d'audit choque : il analyse une situation, mais, comme un devis de réparation, il met l'accent sur les dysfonctionnements pour

faire développer des actions de progrès.

« Au moins une page sur ce qui ne va pas, au plus une ligne sur ce qui va. »

Il contient des recommandations. Une recommandation n'est pas une critique, elle n'implique pas de faute : c'est une solution proposée au responsable habilité à mener l'action. Il est en charge de développer et mettre en place une solution au problème soulevé : celle proposée ou une meilleure.

À réception des formulaires de réponses aux recommandations,
l'Audit :

- **examinera** les programmes d'action décrits, et éventuellement demandera leur modification ;
- **diffusera** l'ensemble des programmes d'action aux principaux destinataires du rapport ;
- **suivra** leur mise en place : émission d'un rapport d'avancement.

AUDIT DE LA SOCIÉTÉ H.A.

RÉSUMÉ

La mission d'audit de la société H.A, effectuée à la demande de la direction générale du groupe, s'est déroulée de janvier à mars 2020. Elle a couvert les trois usines et les services du siège.

La société H.A. réalise un chiffre d'affaires de 200 millions d'euros. Elle élabore et vend des produits destinés à l'industrie. Son siège social est situé à Paris. Elle possède trois usines en Île-de-France qui emploient chacune 200 personnes et achète pour 140 M€ de matières premières.

Le siège s'occupe de tous les aspects financiers et administratifs (gestion de la trésorerie, paie, comptabilité...). Les directeurs d'usine sont responsables du suivi et de la planification de la production.

Les objectifs généraux de la mission étaient d'apprécier la qualité de l'organisation et la maîtrise des opérations d'investissements et d'achats.

Nos remarques détaillées figurent dans le corps du rapport. Elles sont résumées ci-après.

Investissements et achats

Le bien-fondé des engagements d'investissements et des achats de matières premières réalisés par les usines, leur coût et leur rentabilité ne sont pas maîtrisés par la direction de l'entreprise. Des règles communes aux trois usines doivent rapidement être précisées par la direction générale afin de fiabiliser les processus d'investissement et d'approvisionnement (prévision, autorisation, choix de fournisseurs présélectionnés ou appel d'offres, engagement de commande sur la base de conditions financières négociées par le siège, réception, comptabilisation et décaissements).

L'absence de procédure de rapprochement entre les commandes, les bons de réception et la facture ainsi que de contrôle des chèques émis pour régler les factures fournisseurs a entraîné des dépenses ou paiements injustifiés voire en double.

Nous tenons à remercier les personnes contactées au cours de notre mission pour la collaboration qu'elles ont apportée à nos travaux.

A. TRICE et O. DITOSI, auditeurs
Ch. DEMISS, chef de mission
O. SCAR, directeur de l'audit interne

AUDIT DE LA SOCIETE H.A.

CAHIER DES RECOMMANDATIONS – PLAN D'ACTIONS

Le directeur général devrait :

R1 : en liaison avec les directeurs d'usine :

Élaborer un budget des achats en valeur et un budget de réapprovisionnement en quantité, valable pour les trois usines.

Réf. : Approvisionnement des stocks de matières premières : FAR n° 1.

R6 : en liaison avec le directeur financier :

Rédiger une procédure d'investissement prévoyant notamment :

- l'établissement par les directeurs d'usine et la direction de l'entreprise des prévisions d'investissement à long terme liées au budget de production et des ventes ;
- la rédaction par les directeurs d'usine d'un rapport annuel précisant, entre autres, les investissements réalisés par rapport aux investissements budgétés et un résumé sommaire des variations des immobilisations brutes ;
- un seuil d'autorisation au-dessus duquel la demande doit être approuvée à la fois par le directeur d'usine et par la direction de la société, avant l'émission d'un bon de commande ;
- la réalisation par le service comptable d'un rapprochement entre le bon de commande, le bon de réception et la facture avant la comptabilisation et la mise en règlement de celle-ci.

Réf. : Acquisitions d'immobilisations : FAR n° 4.

Les directeurs d'usine devraient :

R2 : Engager des commandes de réapprovisionnement auprès de fournisseurs présélectionnés par le siège dans les conditions financières négociées par le siège.

Respecter, pour chaque commande, le planning de commande/livraison indiqué dans le budget de réapprovisionnement afin d'éviter le surstockage ou la rupture de stock.

Réf : Approvisionnement des stocks de matières premières : FAR n° 1.

Le chef comptable devrait :

R4 : Vérifier que le délai de règlement demandé par le fournisseur coïncide avec celui qui a été négocié.

Réf : Réception des matières premières : FAR n° 2.

R5 : Rédiger une procédure d'autorisation de paiement des factures fournisseur en précisant notamment les opérations à effectuer :

- l'obligation pour le comptable de rapprocher le bon de commande et le bon de réception de la facture avant l'apposition sur la facture d'un « bon à payer », et de joindre la facture au chèque pour signature ;
- l'apposition sur la facture de la mention « payée » par le directeur après la signature du chèque.

Réf : Titre de paiement : FAR n° 3.

Le comptable du siège devrait :

R3 : Recevoir de l'usine un bon de réception établi par le magasinier, précisant clairement la nature, la quantité et la qualité des matières premières réceptionnées.

Comparer les éléments du bon de commande avec ceux de la facture et du bon de réception, puis comptabiliser la facture.

Réf : Réception des matières premières : FAR n° 2.

FAR N° 1 : Approvisionnement des stocks de matières premières

Une gestion économique des approvisionnements (planification, appel d'offres, commande, livraison et suivi budget/ réalisation) et efficace en trésorerie n'est pas assurée.

Constats :

Le délai de livraison des commandes fournisseurs et le nombre de jours de stock sont plus longs pour la société H.A. que la moyenne du secteur.

Des tests réalisés sur 10 fournisseurs par usine ont mis en évidence :

- dans tous les cas, des conditions de paiement moins favorables que la moyenne du secteur ;
- des conditions de paiement différentes accordées par le même fournisseur (société FOUR) aux usines 1 et 3.

Les approvisionnements sont réalisés par les usines de façon irrégulière sur l'année : achats regroupés en avril (32 M€), septembre (21 M€) et octobre (27 M€).

Causes :

Absence de gestion prévisionnelle des stocks.

Absence de procédure de sélection des fournisseurs et d'appel d'offres.

Aucun contrôle n'est réalisé par la direction du siège sur les commandes passées.

Conséquences :

Risques de surstockage ou, au contraire, de rupture de stock.

Risques de paiement trop cher des stocks, de leur livraison lente, et d'obtention de conditions de règlement discutées par chaque directeur d'usine moins favorables que si elles l'étaient par le siège pour les trois usines.

Risque de brusque sortie de trésorerie due à des commandes passées en même temps par les trois usines.

Recommandations :

R1. Le directeur général, en liaison avec les directeurs d'usine, devrait :

Élaborer un budget des achats en valeur et un budget de réapprovisionnement en quantité, valable pour les trois usines. *R2. Les directeurs d'usine devraient :*

Engager des commandes de réapprovisionnement auprès de fournisseurs présélectionnés par le siège dans les conditions financières négociées par le siège.

Respecter, pour chaque commande, le planning de commande/livraison indiqué dans le budget de réapprovisionnement afin d'éviter le sur stockage ou la rupture de stock.

FAR N° 2 : Réception des matières premières

Le traitement des factures fournisseurs présente des faiblesses de contrôle interne et rend possibles des règlements non justifiés.

Constats :

La revue de 30 factures reçues en janvier, février et mars a permis de constater que :

- 10 factures ont été payées alors que la marchandise n'était pas encore reçue ;
- 5 factures ont été payées alors que la marchandise reçue n'était pas conforme à la commande (quantité ou qualité).

Dans deux cas, le fournisseur refuse d'accorder un avoir.

Causes :

Absence d'établissement par le magasinier d'un bon de réception, après réalisation des contrôles nécessaires (nature du bien, quantité, qualité).

Absence de rapprochement entre le bon de commande, le bon de réception et la facture.

Conséquences :

Risque de paiement de factures non justifiées.

Risque de paiement de factures avant l'échéance négociée avec le fournisseur.

Recommandations :

R3. Le comptable du siège devrait :

Recevoir de l'usine un bon de réception établi par le magasinier, précisant clairement la nature, la quantité et la qualité des matières premières réceptionnées.

Comparer les éléments du bon de commande avec ceux de la facture et du bon de réception, puis comptabiliser la facture.

R4. Le chef comptable devrait :

Vérifier que le délai de règlement demandé par le fournisseur coïncide avec celui qui a été négocié.

FAR N° 3 : Titre de paiement

L'absence de procédure de contrôle des chèques émis pour régler les factures fournisseurs entraîne des risques importants de dépenses ou paiements injustifiés voire en double.

Constats :

Un test effectué sur 30 décaissements de montants significatifs relevés dans le journal de banque du mois de mai a mis en évidence :

- l'absence de justificatif pour cinq d'entre eux ;
- le double paiement d'une facture.

Causes :

Les documents justificatifs (facture marquée du rapprochement effectué avec la commande et le BR) ne sont pas joints au chèque (ou ordre de virement) signé par la direction générale.

La mention « payée » n'est pas apposée sur la facture après signature du chèque.

Conséquences :

Risque de paiement de factures n'ayant aucun lien avec les charges de l'entreprise.

Risque de double paiement des factures.

Recommandations :

R5. Le chef comptable devrait :

Rédiger une procédure d'autorisation de paiement des factures fournisseur en précisant notamment les opérations à effectuer :

- l'obligation pour le comptable de rapprocher le bon de commande et le bon de réception de la facture avant l'apposition sur la facture d'un « bon à payer », et de joindre la facture au chèque pour signature ;
- l'apposition sur la facture de la mention « payée » par le directeur après la signature du chèque.

FAR N° 4 : Acquisitions d'immobilisations

Le processus d'investissement (prévision, autorisation, appel d'offres et réception de l'immobilisation) n'est pas fiable. Le bien-fondé, le coût et la rentabilité des investissements ne sont pas maîtrisés par la direction générale.

Constats :

La société H.A. n'établit pas de prévisions d'investissement à long terme.

Aucun investissement n'est autorisé par la direction générale.

L'analyse des dossiers d'investissements réalisés sur l'année a révélé :

- l'absence, dans tous les cas, d'appel d'offres formalisé et de recherche de modes de financements appropriés ;
- le paiement d'une immobilisation non encore livrée à l'usine ;
- le paiement d'une immobilisation pour laquelle des problèmes techniques sont rencontrés.

Causes :

Absence de procédure en matière d'investissement.

Conséquences :

Non-détection de variations anormales des investissements par rapport à l'activité de l'entreprise.

Risque d'acquisition de matériel à un prix trop élevé et de qualité insuffisante et dont le coût de financement viendra encore augmenter le coût d'acquisition de l'immobilisation.

Paiement d'immobilisations non encore livrées ou ne fonctionnant pas correctement.

Recommandations :

R6. Le directeur général, en liaison avec le directeur financier, devrait :

Rédiger une procédure d'investissement prévoyant notamment :

- l'établissement par les directeurs d'usine et la direction de l'entreprise des prévisions d'investissement à long terme liées au budget de production et des ventes ;
- la rédaction par les directeurs d'usine d'un rapport annuel précisant, entre autres, les investissements réalisés par rapport aux investissements budgétés et un résumé sommaire des variations des immobilisations brutes ;
- un seuil d'autorisation au-dessus duquel la demande doit être approuvée à la fois par le directeur d'usine et par la direction de la société, avant l'émission d'un bon de commande ;
- la réalisation par le service comptable d'un rapprochement entre le bon de commande, le bon de réception et la facture avant la comptabilisation et la mise en règlement de celle-ci.

¹. Adaptation du cas d'après *Mémento d'audit interne* (Dunod, 2007) et *Guide d'audit des achats et des ventes* (Eyrolles, 2014).

Conclusion générale

Si nous devons choisir un mot, celui qui pourrait constituer le mot-clé de notre ouvrage, ce serait sans hésiter « risques ». Si nous avons la possibilité de le compléter, ce serait « maîtrise des risques ».

Le management des risques assure l'identification, l'évaluation et le traitement des risques. Le contrôle interne (ou le système de contrôle interne) est la réponse organisationnelle à la maîtrise des risques. La gouvernance, entre autres, structure le fonctionnement des différentes instances chargées de coordonner et piloter la maîtrise des risques. Enfin l'audit, et plus précisément l'audit interne, apprécie l'existence, la bonne application et l'efficacité de tous ces dispositifs. Comme nous l'avons dit de manière un peu caricaturale en introduction, « l'audit, c'est le contrôle du contrôle ».

En matière d'audit interne, le Cadre de référence international des pratiques professionnelles élaboré par l'IIA recense les bonnes pratiques qui garantissent un excellent niveau de qualité aux prestations d'audit réalisées par les services qui s'inscrivent dans cette démarche. La méthodologie que nous préconisons intègre parfaitement les recommandations de ce cadre de référence.

Pour ce qui est du contrôle interne, les modèles préconisés par l'AMF et celui du COSO, plus particulièrement dans sa version actualisée en 2013, constituent actuellement des guides conceptuels incontournables pour définir et mettre en œuvre les dispositifs nécessaires à la maîtrise des risques. Les référentiels de risques proposés dans cet ouvrage s'inspirent de cette logique.

Cependant, et c'est l'objet de toute conclusion d'un ouvrage, nous nous devons d'élargir notre réflexion sur le contrôle des organisations à d'autres dimensions non abordées jusqu'à présent mais qui ne doivent et ne peuvent pas être ignorées.

Le contrôle interne donne une assurance raisonnable quant à la maîtrise des risques de non-atteinte des objectifs (de rentabilité) d'une organisation ; en ce sens, il se préoccupe des intérêts et attentes des actionnaires ou instances de tutelle. Toutefois, il y a d'autres parties prenantes (ou parties intéressées, selon les auteurs) directement concernées par le bon fonctionnement des organisations et qui, à ce titre, ont aussi des attentes spécifiques vis-à-vis de l'organisation. On peut citer :

- les clients qui attendent de l'organisation la satisfaction de leurs besoins lorsqu'ils passent commande ;
- les salariés de l'organisation qui aspirent à une juste rétribution de leur travail, qui doit par ailleurs se dérouler dans des conditions de sécurité satisfaisantes ;
- enfin la société, au sens large, qui exige des organisations un comportement éthique notamment en matière de protection de l'environnement, de développement durable, de lutte contre la corruption, de protection des données des personnes liées à l'activité de l'organisation ou encore de responsabilité « sociétale ».

Concernant les attentes de ces différentes parties prenantes, comme le contrôle interne est une réponse aux attentes des actionnaires, il existe une multitude de réponses (normes, réglementations, lois...) mises en œuvre par les organisations pour y répondre.

Pour les attentes des clients, on parlera des normes qualité ISO 9001. Pour celles des salariés, il s'agira des référentiels OHSAS 18001 et des lois définissant les obligations en matière de santé et de sécurité au travail.

Pour la société au sens large, et concernant le comportement éthique des organisations, il s'agira par exemple de se conformer aux obligations de transparence, de lutte contre la corruption et de modernisation de la vie économique (loi Sapin 2). De même, nous aurons les normes ISO 14000 pour la protection de l'environnement ou celles concernant le développement durable ou encore le « bilan carbone ». Enfin, concernant la protection des données des personnes liées à l'activité de l'organisation (salariés, clients, sous-traitants...), les obligations découlant du RGPD

(Règlement général de protection des données) constitueront la référence en la matière.

La satisfaction des attentes de ces autres parties prenantes constitue, pour l'organisation, des objectifs à atteindre tout aussi importants et légitimes que les objectifs de rentabilité vis-à-vis des actionnaires. Dans la mesure où l'organisation se fixe des objectifs à atteindre, on n'échappe pas à l'enchaînement des étapes que nous avons évoqué dans l'introduction de cet ouvrage : « Objectifs – Risques – Dispositifs de maîtrise des risques – Audit ». On constate donc qu'il existe, parallèlement au système de contrôle interne, divers autres systèmes de management destinés à assurer (autant que faire se peut) la satisfaction des attentes de chaque partie prenante importante pour l'organisation par l'atteinte des objectifs correspondants.

Lors des précédentes éditions de l'ouvrage, nous indiquions que ces divers systèmes de management cohabitaient, se superposaient, étaient parfois en partie redondants sans une véritable volonté d'harmonisation et/ou de vision d'ensemble du problème. Dix ans après, nous relevons de gros progrès tendant à promouvoir un seul système de maîtrise des risques, « intégratif », « équilibré », se préoccupant des objectifs liés aux attentes de toutes les parties prenantes.

Avec la pandémie de 2020 due au coronavirus, cette perspective devient très importante pour l'organisation, voire vitale pour le futur de notre planète.

Elle sera par ailleurs un accélérateur pour développer de nouvelles approches méthodologiques qui favorisent l'audit à distance !

