

Pierre Schick
Jacques Vera
Olivier Bourrouilh-Parège
Préface de Philippe Mocquard

Audit interne et référentiels de risques

**Vers la maîtrise des risques
et la performance de l'audit**

3^e édition

DUNOD


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

<p>Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.</p> <p>Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements</p>	<p>d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.</p> <p>Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).</p>
--	--

DANGER



**LE PHOTOCOPIAGE
TUE LE LIVRE**

© Dunod, 2021

11, rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-081968-3

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.

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'IFACI¹

1. Le contenu de cet ouvrage ne peut engager l'IFACI et reste le fruit de ses auteurs.

Sommaire

Avant-propos	III
Préface	V
Introduction	1

Partie 1 **L'environnement de l'audit interne**

1 Le périmètre d'intervention de l'audit	7
Le gouvernement d'entreprise	8
Le management des risques	10
Le contrôle interne	16
2 La fonction d'audit interne	25
L'audit interne et son évolution	26
Une profession qui s'appuie sur des normes	30
L'Institut français de l'audit et du contrôle internes (IFACI)	34
Les fonctions voisines de l'audit interne	36

3 L'organisation de l'activité d'audit	50
Le rattachement de l'audit interne	51
La charte de l'audit interne	53
L'organisation des moyens	54
La gestion des auditeurs	56
La nécessité de se former	59
La communication de l'audit interne	60
Les mesures de satisfaction et de performance de l'audit	63
4 L'identification des besoins d'audit	65
L'élaboration d'une cartographie des risques	66
L'établissement du plan et du planning d'audit	69

Partie 2

La méthodologie de l'audit

5 Les processus de conduite d'une mission	77
Diagramme global d'une mission d'audit interne	78
Correspondance avec les normes professionnelles du CRIPP	80
Schéma d'une mission pour les audités	80
6 Les modalités d'application (MA)	95
Le droit d'accès : la lettre ou l'ordre de mission	96
L'examen de l'activité et son découpage en « objets auditables »	98
Référentiel d'audit : l'élaboration d'un tableau des risques	104
La réunion d'ouverture ou d'installation de l'équipe	111
L'analyse des forces et faiblesses	113
Le rapport d'orientation ou la note de cadrage	115
Le programme de vérification	117
La conduite des vérifications et la formalisation des travaux de contrôle	119
La fiche d'audit et de recommandations (FAR)	123
L'ossature du rapport	130
Le compte rendu oral sur site	133
Le rapport d'audit et sa validation	135

Le suivi des recommandations	140
L'état des actions de progrès	142
7 Les documents associés (DA)	147
Ordre de mission	148
Tableau des risques	149
Rapport d'orientation	150
Programme de vérification	151
Budget – planning	153
Feuille de couverture de test	154
Feuille de couverture d'entretien	154
Fiche d'audit et de recommandations	155
Projet de rapport d'audit	156
Rapport d'audit	157
Suivi des recommandations / plan d'actions	161
État des actions de progrès	162
Fiche de conseils de perfectionnement post-audit	164
Questionnaire de satisfaction post-audit	166

Partie 3

Les outils de l'audit interne

8 Les techniques d'audit traditionnelles (TA)	173
L'analyse économique et financière	174
Les volumes et types de transactions	176
Les diagrammes de circulation (<i>flow charts</i>)	177
La grille de séparation des tâches	181
Les interviews	185
Les questionnaires administrés	188
La piste d'audit	191
Les observations physiques	193
Les rapprochements et reconstitutions	195
L'interrogation des fichiers informatiques	196
Les sondages statistiques	198

9 Les nouveaux outils liés aux évolutions technologiques	201
Une approche contemporaine de l'audit	202
Une approche des risques intégrant la gestion des autorisations (droits, données et SOD)	204
Les pratiques actuelles et évolutions liées au numérique	206
L'analyse des données (<i>data analytics</i>)	207
L'exploration des données (<i>data mining</i>)	210
L'intelligence artificielle	211
Audit interne et intelligence artificielle (IA)	212
L'apport d'une solution de type hub collaboratif pour piloter un audit interne	213

Partie 4

Les référentiels de risques – illustrations et cas pratiques

10 Les tableaux des risques	219
La structuration et le mode d'utilisation des référentiels	220
Approche globale	223
Approche par processus ou domaines de gestion	240
11 Illustrations et cas pratiques	354
QUIZ	355
Illustrations des 17 principes du COSO	358
Étude de cas : société H.A.	376

Conclusion générale	387
----------------------------	-----

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

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

L'environnement de l'audit interne

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'efficacité 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'expliquer.

« 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

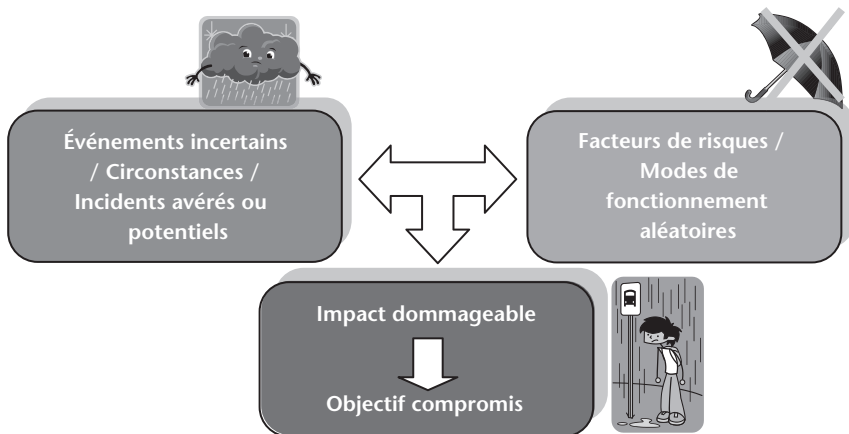


Figure 1.2 – Du concept de risque à sa définition

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 ;