ifaci

institut français de l'audit et du contrôle internes

Cahier de la Recherche

# La cartographie des risques

## 2e édition

*Réalisé par le Groupe Professionnel Assurance*

*L'IFACI est affilié à The Institute of Internal Auditors*

## Dans la même collection

- **De la cartographie des risques au plan d'audit,** Groupe Professionnel « Banque » *(à paraître)*
- **L'audit du versement des subventions aux associations,** Groupe Professionnel « Collectivités Territoriales » *(février 2013)*
- **Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet,** Unité de Recherche Informatique IFACI *(décembre 2012)*
- **L'accès et la conservation des dossiers relatifs aux missions d'audit,** Unité de Recherche IFACI *(octobre 2012)*
- **La délégation de gestion en assurance de personnes : pistes pour un contrôle interne efficace,** Unité de Recherche IFACI *(juin 2012)*
- **Les variables culturelles du contrôle interne,** Unité de Recherche IFACI *(décembre 2011)*
- **Des clés pour la mise en œuvre et l'optimisation du contrôle interne,** Unité de Recherche IFACI *(octobre 2011)*
- **Transposition des normes professionnelles de l'audit interne et bonnes pratiques : Edition spéciale Administrations d'Etat,** Groupe Professionnel « Administrations de l'Etat » *(septembre 2011)*
- **Transposition des normes professionnelles de l'audit interne et bonnes pratiques : Edition spéciale Collectivités Territoriales,** Groupe Professionnel « Collectivités territoriales » *(avril 2011)*
- **La fraude : Comment mettre en place un dispositif de lutte contre la fraude ?** Unité de Recherche de l'IFACI *(décembre 2010)*
- **La création de valeur par le contrôle interne,** Unité de Recherche de l'IFACI *(octobre 2010)*
- **Prise de Position du Groupe Professionnel Banque pour un urbanisme du contrôle interne efficient,** Groupe Professionnel « Banque » *(Avril 2010)*
- **L'audit de la fraude dans le secteur bancaire et financier,** Unité de Recherche de l'IFACI *(janvier 2010)*
- **Création et gestion d'une petite structure d'audit interne,** Unité de Recherche IFACI *(janvier 2009)*
- **Une démarche d'audit de plan de continuité d'activité,** Unité de Recherche IFACI *(juillet 2008)*
- **Guide d'audit du développement durable : comment auditer la stratégie et les pratiques de développement durable ?,** Unité de Recherche IFACI *(juin 2008)*
- **Contrôle interne et qualité : pour un management intégré de la performance,** Unité de Recherche IFACI *(mai 2008)*
- **Evaluer et développer les compétences des collaborateurs,** Antenne régionale Aquitaine IFACI *(novembre 2007)*
- **Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement– 2ème Edition,** Groupe Professionnel « Banque » *(janvier 2007)*
- **L'audit interne et le management des collectivités territoriales,** Unité de Recherche IFACI *(mai 2006)*
- **Une démarche de management des connaissances dans une direction d'audit interne,** Unité de Recherche IFACI *(mai 2006)*
- **L'auto-évaluation du contrôle interne,** Unité de Recherche IFACI *(octobre 2005)*
- **Cartographie des Risques,** Groupe Professionnel « Immobilier Locatif » *(septembre 2005)*
- **Étude du processus de management et de cartographie des risques,** Groupe Professionnel « Industrie et commerce » *(janvier 2004)*
- **Pour un bon audit du dispositif de lutte contre le blanchiment des capitaux,** Groupe Professionnel « Banque » *(février 2004)*
- **L'efficacité des Comités d'audit – Les meilleures pratiques,** PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Gouvernement d'entreprise et Conseil d'administration,** PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Évaluation de la compétence dans la pratique de l'audit interne,** Prise de position de l'ECIIA – Traduction IFACI *(2001)*
- **Management des risques,** IIA UK – Traduction Unité de Recherche IFACI *(2001)*
- **Le rôle de l'auditeur interne dans la prévention de la fraude,** Prise de position de l'ECIIA – Traduction IFACI *(2000)*

Pour plus d'informations : www.ifaci.com



© IFACI

# Remerciements

L'IFACI tient à remercier toutes les personnes qui ont contribué aux différentes étapes de l'élaboration de ce Cahier.

- **Pilotage et revue d'ensemble :**
  **Groupe professionnel « Assurance » de l'IFACI,** présidé par **Anne SAVEY,** *Responsable Contrôle Général, Groupe MMA*

- **Animation et rédaction :**
  **Philippe BERTOMEU,** *Manager Audit interne, Axa France*
  **Wilfried BRIAND,** *Chargé de mission du Directeur Général, CNP Assurances*
  **Michel BUZEJIC,** *Responsable Audit interne, Quatrem, animateur de l'unité de recherche*
  **Guillaume KUCH,** *Responsable du service pilotage des Clientèles Bancaires, CNP Assurances*
  **Eric LHUISSIER,** *Responsable Contrôle interne et conformité, MMA*
  **Alain MARTEL,** *Directeur de la Maîtrise des Risques, MATMUT*
  **Lamyaa NADARI,** *Auditeur interne / Inspecteur, Allianz IARD*
  **Marine NGUYEN,** *Responsable du département de politique indemnisation et contrôle interne, Generali*
  **Emmanuel RUFFIN,** *Responsable Contrôle interne et Conformité, MATMUT*
  **Christelle SAINATO,** *Responsable de la Maîtrise des Risques, Harmonie Mutuelle*
  **Patrick SAINT-MAXENT,** *Responsable Pilotage des risques opérationnels et Qualité, AG2R LA MONDIALE*
  **Raphael SIFFERT,** *Coordinateur de contrôle permanent, BNP Paribas Cardif*

  L'unité de recherche remercie **Marina CRISTOFARI**, *Compliance & Control, BNP Paribas Assurance,* **Sébastien SAIDANE,** *Responsable de module de Risque, MATMUT* et **Fabienne VIBOUD,** *Manager Audit interne, COFACE* pour leur contribution.

- **Comité de rédaction et de révision :**
  **Michel BUZEJIC,** *Responsable Audit interne, Quatrem, animateur de l'unité de recherche*
  **Vianney DUMONT,** *Responsable Audit interne, MAIF, Représentant du GP Assurances de l'IFACI*
  **Béatrice KI-ZERBO,** *Directeur de la Recherche, IFACI*
  **Alain MARTEL,** *Directeur de la Maîtrise des Risques, MATMUT*
  **Patrick SAINT-MAXENT,** *Responsable Pilotage des risques opérationnels et Qualité, AG2R La Mondiale*
  **Raphael SIFFERT,** *Coordinateur de contrôle permanent, BNP Paribas Cardif*

- **Organisation des réunions et mise en forme du document :**
  **Perrine BÉNARD,** *Documentaliste, IFACI*
  **N'Della YATERA,** *Chargée de missions Recherche, IFACI*

**Philippe MOCQUARD,** *Délégué Général, IFACI*

© IFACI

# Sommaire

INTRODUCTION ..... 7

1- L'EXERCICE DE CARTOGRAPHIE DES RISQUES :
ETAT DES LIEUX ET PERSPECTIVES ..... 9

1.1- Retour d'expérience des membres de l'unité de recherche ..... 10

1.2- Cadres normatifs et réglementaires ..... 11

1.3- Cadre spécifique aux activités d'assurance ..... 14

1.3.1- Les décrets relatifs au contrôle interne ..... 14

1.3.2- Les attentes de l'Autorité de Contrôle Prudentiel (ACP) ..... 15

1.3.3- La directive *Solvabilité II* ..... 17

2- ACTEURS ET GOUVERNANCE ..... 19

2.1- Les acteurs-clés de la cartographie des risques ..... 20

2.1.1- Les fonctions opérationnelles ..... 21

2.1.2- Les fonctions support de maîtrise des risques ..... 21

2.1.3- L'audit interne ..... 23

2.1.4- En synthèse : six étapes clés et des responsabilités clairement définies ..... 24

2.2- Les instances de gouvernance ..... 25

2.2.1- Organe d'administration, de gestion ou de contrôle ..... 25

2.2.2- Gouvernance institutionnelle : comité d'audit et/ou des risques ..... 26

2.2.3- Gouvernance opérationnelle : comité managérial des risques ..... 26

2.2.4- Autres comités internes participant à la gestion des risques dans le cadre de décisions opérationnelles ..... 27

3- IDENTIFICATION ET EVALUATION DES RISQUES ..... 29

3.1- La notion de risque ..... 30

3.1.1- Définitions ..... 30

3.1.2- Appétence pour les risques et seuil de tolérance ..... 31

3.1.3- La nomenclature des risques ..... 32

3.2- Mesure du risque ..... 35

3.2.1- La fréquence ..... 36

3.2.2- L'impact ..... 37

3.2.3- Le risque brut ..... 39

3.2.4- Les éléments de maîtrise ..... 39

3.2.5- Le risque résiduel ..... 40



© IFACI

3.3- Deux approches complémentaires ..... 41
3.3.1- L'approche *bottom-up* ..... 41
3.3.2- L'approche *top-down* ..... 46
3.3.3- Intégration des deux démarches ..... 47
**4- SUIVI PERMANENTDES RISQUES ..... 53**
4.1- Une modalité particulière de suivi à partir de la base d'incidents ..... 54
4.2- Une communication appropriée ..... 55
4.2.1- *Reporting* interne ..... 56
4.2.2- *Reporting* externe ..... 59
**CONCLUSION ..... 61**
**ANNEXES ..... 63**
1- Exemples de processus - Secteur assurances ..... 64
2- Nomenclature des risques ..... 65
3- Présentation des risques de la formule standard du calcul du SCR ..... 109
4- Exemple d'impact financier ..... 118
5- Evaluation de l'impact financier d'un incident ..... 119
6- Illustration - Synthèse du processus de collecte des événements ..... 122
7- Directive *Solvabilité II* (Extraits) ..... 123
8- Décret n°2006-287 du 13 mars 2006 relatif au contrôle interne des entreprises d'assurance et modifiant le Code des assurances (Extraits) ..... 127
9- Décret n°2008-468 du 19 mai 2008 relatif au contrôle interne des institutions de prévoyance, des mutuelles et de leurs unions ..... 128
10- Exemple de *reporting* ..... 130
**BIBLIOGRAPHIE ..... 135**

© IFACI

**Avertissement aux lecteurs**

Ce cahier de la recherche a été réalisé à partir de contributions de professionnels de l'audit et du contrôle internes. Ce travail collectif, réalisé sous l'égide de l'IFACI, fournit un état des lieux des pratiques professionnelles et des pistes d'amélioration qui n'engagent pas les organisations représentées.

L'Autorité de Contrôle Prudentiel (ACP) est devenue l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) par la loi n° 2013-672 du 26 juillet 2013, de séparation et de régulation des activités bancaires. Le présent ouvrage rédigé durant le 1er semestre 2013, n'a donc pas intégré ce changement de dénomination.

© IFACI – Paris – septembre 2013 ISBN : 978-2-915042-56-6 – ISSN : 1778-7327

*Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droits, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.*



© IFACI

# Introduction

Le premier ouvrage du Groupe Professionnel « Assurance » de l'IFACI, publié en 2006, a été un outil de référence pour la sensibilisation aux démarches de cartographie des risques ou pour leur mise en œuvre. Ainsi, il a pu être utilisé dans des organismes d'assurance qui formalisaient leur dispositif de contrôle interne (notamment dans le cadre de la Loi de Sécurité Financière, ou Sarbanes-Oxley), mais également accompagner ceux qui ont engagé des démarches globales de gestion des risques du type ERM *(Entreprise Risk Management)*.

Les évolutions réglementaires constantes, les demandes de plus en plus précises de la part du superviseur, l'intérêt croissant des instances de gouvernance ainsi que la volonté de faire progresser la maîtrise des risques de chaque organisme d'assurance ont conduit le Groupe Professionnel « Assurance » à actualiser le cahier de la recherche.

Cette mise à jour a pu s'appuyer sur la diversité des métiers (contrôle interne, gestion des risques, audit interne) représentés dans l'unité de recherche pour identifier les axes d'amélioration des démarches de cartographies des risques existantes, notamment dans la perspective de la mise en œuvre de la directive *Solvabilité II*.

L'unité de recherche a fonctionné de façon pragmatique et collégiale. Pragmatique dans la mesure où chacun y a participé sur une base volontaire afin d'y apporter sa propre expérience et s'enrichir de celle des autres participants. Collégiale car il s'agissait de définir de façon consensuelle la position du groupe de travail.

Les travaux se sont déroulés en 2012, les contributeurs ont notamment :

- tenu compte de l'évolution du niveau de maturité des démarches de cartographie des risques et des retours d'expériences partagées,
- mieux pris en compte les risques économiques, de solvabilité, et de réputation dans la mise à jour de la typologie des risques,
- précisé les rôles des acteurs des démarches de cartographie des risques et les responsabilités des organes de gouvernance,
- mis l'accent sur le *reporting* approprié permettant à chacun de ces acteurs de jouer efficacement leur rôle,
- attiré l'attention sur la nécessaire intégration de la cartographie des risques dans le dispositif de maîtrise des risques (lien avec les bases d'incidents, les plans d'actions, etc.),
- fait références aux risques spécifiques (blanchiment, protection de la clientèle, etc.) et à leur prise en compte dans la démarche globale de cartographie des risques,
- introduit les principes théoriques de l'ORSA (qui sont en cours de mise en œuvre actuellement) et leur impact sur les pratiques de cartographie des risques.

© IFACI

En proposant des clés de lecture et des guides méthodologiques pour chaque étape de la cartographie des risques, ce cahier de la recherche permettra aux différents acteurs des organismes d'assurance d'appréhender leur rôle dans ce processus. D'un abord didactique, il n'est pas réservé aux experts de la maîtrise des risques. En effet, la cartographie des risques n'est pas une fin en soi. Les membres des organes exécutifs et les administrateurs y trouveront des principes fondamentaux pour assumer leurs responsabilités de surveillance de ces démarches et assurer leur intégration efficace au processus global de gestion des risques.



© IFACI

# Partie 1

# L'exercice de cartographie des risques : état des lieux et perspectives

Le présent cahier de la recherche s'inscrit dans le prolongement de la première publication du Groupe Professionnel « Assurance » de l'IFACI. Il prend en compte les bonnes pratiques résultant des travaux de cartographie des risques dans les organismes d'assurance depuis 2006. Il s'intègre également dans la perspective de la mise en œuvre de la directive *Solvabilité II*. Néanmoins, les propositions formulées à cet égard devront sans doute être revisitées compte tenu du niveau de déploiement de cette directive à la date de finalisation du cahier.

© IFACI

## 1.1 Retour d'expérience des membres de l'unité de recherche

Un *benchmark* portant sur les démarches de cartographies des risques montre que 83% des organismes d'assurance représentés dans l'unité de recherche ont utilisé la première édition du cahier de la recherche, aussi bien pour la mise en place des cartographies des risques que pour leurs actualisations.

Il est utilisé par différentes entités : directions des risques, directions de contrôle interne ou directions de l'audit interne. Ces dernières l'utilisent dans le cadre de l'élaboration du plan d'audit ou des programmes de travail d'une mission.

Les principaux apports mentionnés par les utilisateurs concernent la description pédagogique de la méthodologie ainsi que la nomenclature des risques.

Les premières démarches structurées et formalisées de cartographies des risques ont été mises en place à partir de 2003 généralement pour répondre aux exigences de la Loi Sarbanes-Oxley, de la Loi de Sécurité Financière et du décret du 13 mars 2006 relatif au contrôle interne des entreprises d'assurance[1]. Depuis 2010, des démarches complémentaires ont été initiées pour notamment assurer le suivi des risques dits « majeurs ». Ainsi, certains organismes d'assurance peuvent disposer de plusieurs types de représentation de leurs risques.

Conformément à la nomenclature proposée en 2006, les principales familles de risques concernent les risques opérationnels, les risques financiers, les risques d'assurance et techniques. Les risques stratégiques ou les risques externes (par exemple : évolutions réglementaires, risque pays, concurrence, etc.) sont peu mentionnés. Pourtant, ils font partie des préoccupations majeures des directions générales des organismes d'assurance.

Dans 54% des cas, l'élaboration des cartographies des risques est centralisée au niveau d'une entité dédiée aux risques, qui donne la méthodologie, la trame, l'impulsion. La responsabilité de leur suivi incombe aux directions et/ou entités opérationnelles, qui peuvent être amenées à nommer un « correspondant risques ». Ce dispositif s'est mis en place progressivement dans les organismes et traduit une certaine maturité sur ces sujets. Il concerne principalement les risques opérationnels et/ou les processus métiers.

La communication et le *reporting* sont principalement à destination du management des entités, des fonctions « risques », du « contrôle interne », de l'audit interne et des comités d'audit ou des risques. Le niveau et le format de restitution sont déclinés en fonction de cette diversité de destinataires.

[1] *Cf. Article R336-1 du code des assurances.*



© IFACI

48% des organismes ont fait l'acquisition ou ont développé des progiciels dédiés à la maîtrise des risques[1]. La mise en place de tels outils peut faciliter une vision intégrée de différents éléments de la maîtrise des risques (cartographies des risques, plans d'actions, suivi des incidents, recommandations des audits internes et externes, etc.).

Les avancées réalisées par le secteur et la professionnalisation croissante des acteurs de la maîtrise des risques sont notables. Elles s'insèrent dans le cadre d'une évolution générale des organisations et d'exigences spécifiques au secteur de l'assurance (notamment les exigences des autorités de tutelle et de la directive *Solvabilité II*).

## 1.2 Cadres normatifs et réglementaires

Historiquement, les pratiques de cartographies des risques ont été portées par les projets de contrôle interne. Si le contrôle interne est un sujet assez ancien, les crises (Enron, WorldCom ou Parmalat) du début des années 2000, ont donné naissance à des réglementations dans de nombreux pays, et ont contribué à renforcer les pratiques de contrôle interne et de maîtrise des risques au sens large.

Ainsi, la loi Sarbanes Oxley, votée en 2002, requiert que les sociétés cotées à New York documentent les dispositifs de contrôle interne des processus conduisant à l'établissement des états financiers. Testés par les opérationnels eux-mêmes, l'existence et le bon fonctionnement de ces dispositifs sont attestés par les commissaires aux comptes. La mise en œuvre de cette loi s'est clairement appuyée sur le référentiel COSO dont l'une des composantes-clés[2] concerne l'évaluation des risques.

Votée en 2003, la loi de sécurité financière s'inscrit également dans cette volonté de renforcer la transparence et le contrôle interne des entreprises cotées. En 2006, l'AMF (Autorité des Marchés Financiers) propose aux émetteurs un cadre de référence de contrôle interne. Compatible avec les principes du COSO, le cadre de référence a été actualisé en 2010 pour intégrer les exigences de la 8ème directive européenne en matière de suivi de l'efficacité des systèmes de gestion des risques et de contrôle interne par les comités d'audit.

---

[1] *Cf. Cahier de la recherche « Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet » et la revue Audit & Contrôle Internes - Ifaci - N°212 - Novembre / décembre 2012.*

[2] *Les 5 composantes interdépendantes du contrôle interne proposé par le COSO sont : l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, les activités de pilotage. Le COSO définit le contrôle interne comme* un processus mis en œuvre par le Conseil, le management et les collaborateurs, et qui est destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité.

© IFACI

**« Un processus de gestion des risques comprenant, au sein de son contexte interne et externe à la société, trois étapes :**

- **Identification des risques :** étape permettant de recenser et de centraliser les principaux risques, menaçant l'atteinte des objectifs. Un risque représente une menace ou une opportunité manquée. Il se caractérise par un événement, une ou plusieurs sources et une ou plusieurs conséquences. L'identification des risques s'inscrit dans une démarche continue.

- **Analyse des risques :** étape consistant à examiner les conséquences potentielles des principaux risques (conséquences qui peuvent être notamment financières, humaines, juridiques, ou de réputation) et à apprécier leur possible occurrence. Cette démarche est continue.

- **Traitement du risque :** étape permettant de choisir le(s) plan(s) d'action le(s) plus adapté(s) à la société. Pour maintenir les risques dans les limites acceptables, plusieurs mesures peuvent être envisagées : la réduction, le transfert, la suppression ou l'acceptation d'un risque. Le choix de traitement s'effectue notamment en arbitrant entre les opportunités à saisir et le coût des mesures de traitement du risque, prenant en compte leurs effets possibles sur l'occurrence et/ou les conséquences du risque. »

*Cf. Les dispositifs de gestion des risques et de contrôle interne : cadre de référence / AMF. - 2010.*

D'autres référentiels de gestion des risques proposent des définitions et des principes dont l'unité de recherche s'est inspirée :

## • *Le management des risques de l'entreprise : COSO 2*

Le référentiel publié par le COSO en 2004 promeut la notion de gestion globale des risques de l'entreprise, l'*Enterprise Risk Management* ou ERM ; dont l'un des enjeux consiste à amener l'entreprise à aligner sa stratégie et sa gestion des risques. Ainsi, ce référentiel (COSO 2) reprend les trois objectifs et les cinq composantes du référentiel relatif au contrôle interne, qu'il complète avec la prise en compte des objectifs stratégiques et de trois composantes supplémentaires :

- la fixation des objectifs,
- l'identification des événements,
- le traitement des risques selon les 4 modalités classiques (l'évitement, l'acceptation, la réduction, le partage).

Ces principes permettent de repositionner la cartographie des risques dans un dispositif plus global de pilotage des activités. Il nécessite une identification préalable des niveaux de risque acceptables au regard d'objectifs (par exemple : profiter de nouvelles opportunités, conserver des avantages) définis par les instances dirigeantes et déclinés à tous les niveaux de l'organisation.



© IFACI

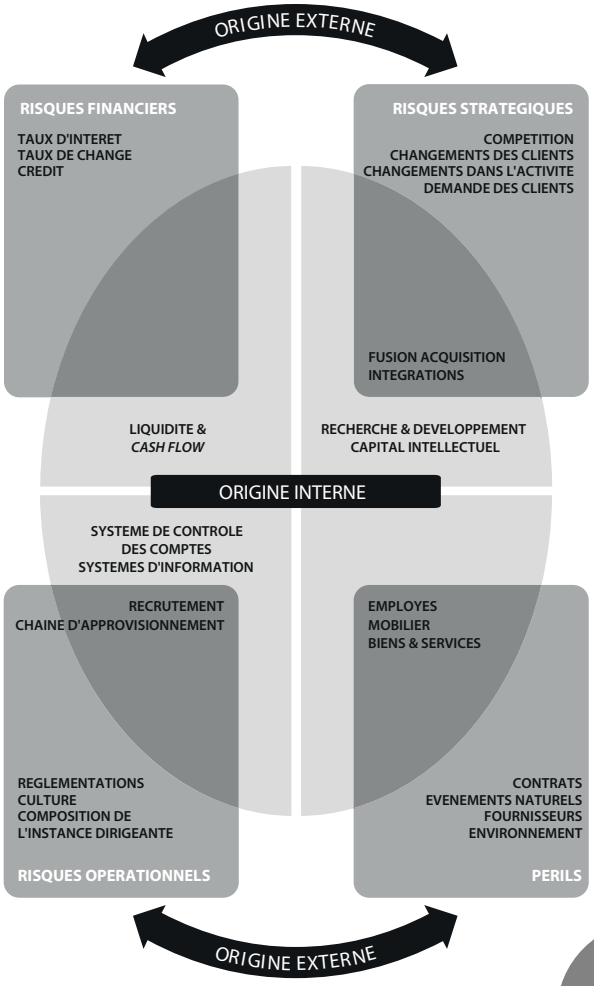
## • *ISO 31000 : 2009*

La norme ISO 31000 vise également un management global des risques. Elle propose de faire de ce dispositif un véritable outil d'aide à la décision.
La norme ISO 31010 : 2009 relative aux techniques d'évaluation des risques précise l'intérêt de ces approches pour :

- appréhender les risques et leurs impacts potentiels sur les objectifs,
- fournir des informations aux décideurs et les aider à établir des priorités,
- aider à la sélection de mesures de traitement appropriées,
- identifier les principaux facteurs de risques au sein des systèmes de gestion et des organisations,
- comparer des options d'organisation, de déploiement de technologies,
- contribuer à la prévention des incidents par une meilleure compréhension des facteurs déclencheurs et des impacts,
- répondre à des exigences réglementaires,
- s'assurer que les niveaux de risque correspondent aux seuils acceptés par l'organisation.

## • *FERMA*

Le FERMA *(Federation of European Risk Management Associations)* propose un cadre de référence de la gestion des risques (2003) et organise les facteurs de risques internes et externes comme suit :




*Exemples de facteurs internes et externes (extrait de Gestion des risques / FERMA. – 2003)*

© IFACI

## 1.3 Cadre spécifique aux activités d'assurance

Des exigences propres au secteur de l'assurance viennent préciser les attentes en matière de contrôle interne et de gestion des risques.

### 1.3.1 Les décrets relatifs au contrôle interne

#### *1.3.1.1 Le décret du 13 mars 2006 relatif au contrôle interne des entreprises d'assurance*

« Toute entreprise mentionnée à l'article L. 310-1 du code des assurances est tenue de mettre en place un dispositif permanent de contrôle interne. Le conseil d'administration ou le conseil de surveillance approuve, au moins annuellement, un rapport sur le contrôle interne, qui est transmis à l'Autorité de Contrôle Prudentiel (cf. annexe 8). [...] Toutefois, les entreprises faisant appel public à l'épargne ne sont pas tenues de fournir ces éléments lorsqu'elles transmettent à l'Autorité de Contrôle Prudentiel le rapport mentionné, selon les cas, à l'article L. 225-37[1] ou à l'article L. 225-68 du code de commerce. »

#### *1.3.1.2 Le décret du 19 mai 2008 relatif au contrôle interne des institutions de prévoyance, des mutuelles et de leurs unions*

**Pour les institutions de prévoyance ou unions :** Toute institution ou union mentionnée à l'article R. 931-43 du code de la sécurité sociale est tenue de mettre en place un dispositif permanent de contrôle interne. Le conseil d'administration approuve, au moins annuellement, un rapport sur le contrôle interne, qui est transmis à l'Autorité de Contrôle Prudentiel.

**Pour les mutuelles ou unions :** Toute mutuelle ou union mentionnée à l'article R. 211-28 du code de la mutualité est tenue de mettre en place un dispositif permanent de contrôle interne. Le conseil d'administration approuve, au moins annuellement, un rapport sur le contrôle interne, qui est transmis à l'Autorité de Contrôle Prudentiel. Un extrait du décret est proposé en annexe 9.

---

[1] *Dans les sociétés dont les titres financiers sont admis aux négociations sur un marché réglementé, le président du conseil d'administration rend compte, dans un rapport joint au rapport mentionné aux articles L. 225-100, L. 225-102, L. 225-102-1 et L. 233-26, de la composition du conseil et de l'application du principe de représentation équilibrée des femmes et des hommes en son sein, des conditions de préparation et d'organisation des travaux du conseil, ainsi* ***que des procédures de contrôle interne et de gestion des risques mises en place par la société, en détaillant notamment celles de ces procédures qui sont relatives à l'élaboration et au traitement de l'information comptable et financière pour les comptes sociaux et, le cas échéant, pour les comptes consolidés.*** *Sans préjudice des dispositions de l'article L. 225-56, ce rapport indique en outre les éventuelles limitations que le conseil d'administration apporte aux pouvoirs du directeur général.*



© IFACI

## 1.3.2 Les attentes de l'Autorité de Contrôle Prudentiel (ACP)

Par ses instruments juridiques et ses contrôles permanents, l'Autorité de Contrôle Prudentiel (ACP) donne des orientations qu'il convient de prendre en considération dans l'exercice de cartographie des risques.

### *1.3.2.1 Les recommandations et les positions de l'ACP*

En complément des textes législatifs et réglementaires, l'ACP émet des positions ou des recommandations à destination des organismes soumis à son contrôle et au public. L'ACP crée ainsi un droit souple ou *soft law* pour exercer ses missions d'analyse et de contrôle concernant :

- l'application des lois et des règlements en matière prudentielle,
- la vigilance permanente en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT),
- le respect des règles en matière de commercialisation de produits et protection de la clientèle.

L'ACP publie un recueil de l'ensemble des codes de conduite, règles professionnelles et autres bonnes pratiques constatées ou recommandées dont elle assure le respect *(article L612-29-1 du code monétaire et financier)*. Les organismes d'assurance sont donc tenus d'intégrer ces positions et recommandations afin de se couvrir de tout risque de non-conformité ou d'image.

*Schéma récapitulatif du corpus de textes de l'ACP*

© IFACI

### 1.3.2.2 Le contrôle permanent de l'ACP

L'ACP veille à ce que les organismes d'assurance soient en mesure de tenir à tout moment les engagements qu'ils ont pris envers leurs assurés, adhérents et bénéficiaires, et qu'ils les tiennent effectivement.

Pour mener à bien ses missions, l'ACP s'appuie notamment sur des diagnostics individualisés pour chaque organisme. A titre d'illustration, 531 organismes d'assurance ont fait l'objet d'une évaluation de leur profil de risque (cf. Rapport d'activité annuel 2011 de l'ACP).
Ces évaluations portent sur les domaines suivants :

- **Le risque de souscription :**
  - engagements pris envers les assurés, adhérents et bénéficiaires des contrats,
  - tarification,
  - surveillance du portefeuille,
  - adaptation de la politique de réassurance.
- **La qualité et la suffisance des provisions :**
  - taux d'actualisation et table employés,
  - évolution de la fréquence des sinistres et des coûts moyens,
  - suivi des sinistres graves.
- La diversification suffisante et **l'évaluation prudente des placements :**
  - classement réglementaire,
  - comptabilisation des dépréciations durables nécessaires,
  - constitution de provision complémentaire le cas échéant.
- **Le risque opérationnel** lié notamment au :
  - risque de fraude ou d'erreur,
  - déficience des systèmes d'information,
  - risque de réputation.
- La qualité de la **gestion actif-passif** et de la gestion du **risque de taux d'intérêt**.
- La qualité de l'organisation du dispositif de conformité et de **contrôle interne**, incluant les **modalités de surveillance et de maîtrise des risques**.
- **La gouvernance d'entreprise** et le fonctionnement régulier des organes délibérants et dirigeants.
- La rentabilité des opérations d'assurance et la formation du résultat.
- Le niveau, la structure et la pérennité des fonds propres.

La situation de chaque organisme est analysée en se fondant sur :

- des données quantitatives au regard de chacun des critères d'évaluation, ainsi que de sa situation financière ;
- des données qualitatives visant à évaluer la qualité du dispositif de surveillance et de maîtrise des risques.


© IFACI

### 1.3.3 La directive *Solvabilité II*

Afin de garantir la capacité des organismes d'assurance à respecter les engagements qu'ils prennent auprès de leurs clients, la directive *Solvabilité II*[1] poursuit plusieurs objectifs :

- assurer la protection des assurés en renforçant la solvabilité des assureurs ;
- encourager une meilleure allocation des fonds propres face aux risques techniques, financiers, opérationnels, etc.

Pour ce faire, la directive retient une approche articulée autour de trois piliers :

- **Pilier 1 - Exigences quantitatives :**
  - éléments de calculs des provisions techniques,
  - exigence minimale de fonds propres,
  - exigence de marge de solvabilité,
  - règles d'investissement.

- **Pilier 2 - Exigences qualitatives de bonne gouvernance :**
  - règles d'honorabilité et de compétence,
  - fonctions clés (de gestion des risques, de vérification de la conformité, actuarielle, d'audit interne),
  - évaluation interne du risque et de la solvabilité (ORSA – *Own Risk and Solvency Assessment*).

- **Pilier 3 - Discipline de marché par une information régulière des autorités de surveillance et du public :**
  - communication financière,
  - transparence.

Les travaux de l'unité de recherche s'intègrent plus particulièrement dans le cadre du Pilier 2, même si une interaction existe avec les autres piliers. En effet, les fonctions clés participent activement à la démarche. De même, la cartographie des risques viendra alimenter l'ORSA.

[1] *Directive 2009/138/CE du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II).*

© IFACI

© IFACI

# Partie 2

# Acteurs et gouvernance

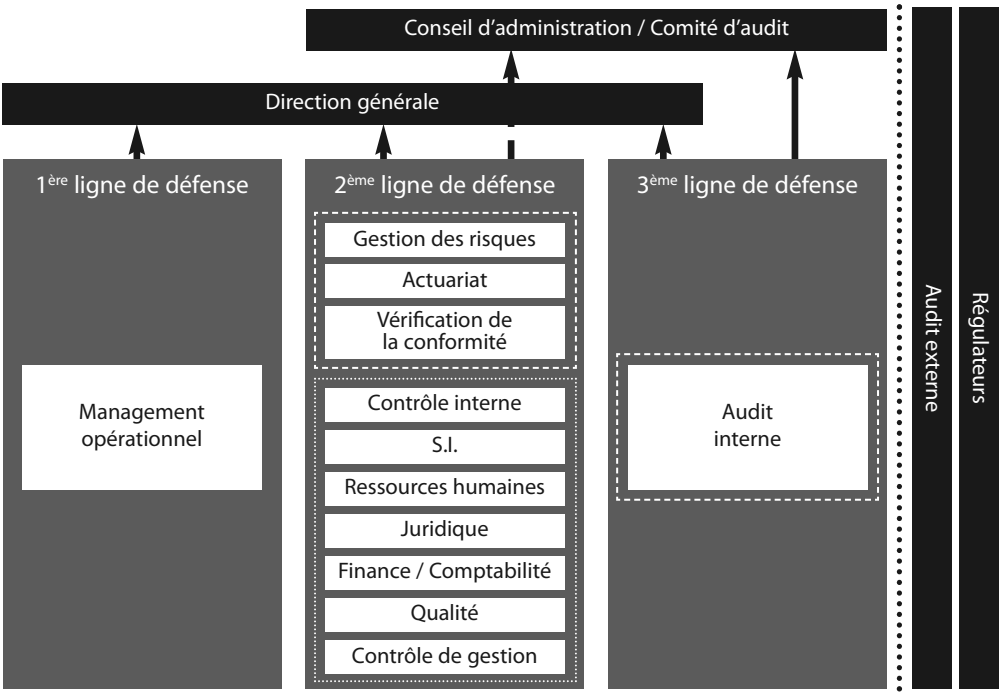
La gouvernance de la gestion des risques présente une dimension stratégique et une dimension opérationnelle, permettant une répartition claire et une séparation appropriée des responsabilités des acteurs impliqués.

Un certain nombre d'acteurs est amené à intervenir dans l'exercice de cartographie des risques, en qualité de « sponsor », de « coordinateur », de « contributeur », « d'utilisateur ». L'allocation précise de ces rôles devrait être cohérente avec le modèle des trois lignes de défense (ou des lignes de maîtrise) et le modèle d'organisation de chaque organisme d'assurance.

© IFACI

## 2.1 Les acteurs-clés de la cartographie des risques

En termes d'organisation, la directive et les documents associés instituent des fonctions clés. En outre, des organisations professionnelles (ECIIA/FERMA, IIA, AMRAE /IFACI) proposent un pilotage efficient des dispositifs de gestion des risques en s'appuyant sur trois lignes de défense, représentées dans le modèle suivant :




Légende : Fonctions clés (SII)
Autres fonctions support

Positionnement et rôles de chaque ligne de défense dans les systèmes de gestion des risques et de contrôle interne :

- la première ligne de défense correspond aux contrôles pilotés par le management opérationnel ou métier,
- la deuxième ligne de défense est celle des différentes fonctions instituées par les organisations pour assurer le contrôle et le suivi des risques. Les fonctions clés définies par la directive *Solvabilité II* bénéficient d'une certaine autonomie voire indépendance, par rapport aux activités opérationnelles / métiers afin de garantir la fiabilité de leurs évaluations des


© IFACI

risques, l'adéquation de leurs propositions de plans de remédiation et leur suivi. En tant que fonctions support du management, elles peuvent directement intervenir dans la modification et la mise au point des systèmes de contrôle interne et de gestion des risques à la différence de l'audit interne.
Outre les fonctions clés, des fonctions support plus traditionnelles participent à la deuxième ligne de défense (directions financières, informatiques, ressources humaines, juridique, qualité, etc.) ; elles-mêmes amenées à émettre des politiques et/ou directives applicables au sein des organisations ; elles assurent également des activités de contrôles.

- la troisième ligne de défense est celle de l'assurance indépendante fournie par l'audit interne. De plus, l'audit interne bénéficie de règles déontologiques et professionnelles qui confortent son indépendance et son objectivité.

L'unité de recherche a choisi de préciser les rôles des acteurs de la cartographie des risques en partant de ce modèle.

### 2.1.1 Les fonctions opérationnelles

La première ligne regroupe les opérationnels (par exemple, les directions métiers chargées de la gestion des contrats d'assurance, des sinistres, des cotisations, etc.). Leur connaissance des métiers les place dans un rôle incontournable dans l'identification des risques inhérents à leur activité, la maintenance de cette cartographie des risques, sa primo-évaluation et le déploiement des contrôles-clés destinés à maîtriser les risques identifiés.

Ainsi, le management a la responsabilité de la maîtrise des risques sur son périmètre. Il examine les expositions de risques, définit les priorités à la lumière de l'analyse des risques. Il doit promouvoir la sensibilité aux risques dans les unités et faire connaître les objectifs de gestion des risques.

### 2.1.2 Les fonctions support de maîtrise des risques

Le suivi des risques, effectué par les directions opérationnelles et les structures de contrôles hiérarchiques, est renforcé par les activités de la deuxième ligne de défense dans laquelle se retrouvent les fonctions clés gestion de risques, actuarielle et de vérification de la conformité.

#### *2.1.2.1 La fonction gestion des risques*

Celle-ci veille à ce que le niveau de risque pris par l'organisme d'assurance, soit cohérent avec les orientations[1] et les objectifs définis par les organes d'administration, de gestion, de contrôle. Ainsi,

[1] *La stratégie, la politique des risques en particulier le niveau d'appétit pour les risques et les seuils de tolérance.*

© IFACI

la fonction « gestion des risques » propose aux dirigeants un profil des risques de l'organisme, à travers :

- une vision holistique des risques de l'organisme,
- une perspective élargie lors de la prise de décisions stratégiques,
- des plans de maîtrise des risques.

Elle anime l'ensemble du dispositif d'identification, de mesure, de traitement, de surveillance et de *reporting* des risques, notamment ceux énoncés par la directive *Solvabilité II*.

#### 2.1.2.2 La fonction actuarielle

La fonction « actuarielle » contribue à l'amélioration du système de gestion des risques. Elle donne avec objectivité une opinion aux organes dirigeants et délibérants, sur la fiabilité et le caractère adéquat du calcul des provisions techniques (opinion et marge d'incertitude), sur les politiques de souscription et les dispositifs de réassurance. Dans ce cadre, elle établit un rapport annuel à destination des organes dirigeants et délibérants. A noter que le document de travail du CEIOPS « CP58[2] » précise que la fonction actuarielle doit disposer d'un niveau suffisant d'indépendance fonctionnelle.

#### 2.1.2.3 La fonction de vérification de la conformité

La fonction de « vérification de la conformité » veille au respect des obligations découlant des dispositions légales et réglementaires, des normes professionnelles et déontologiques ainsi que des règles internes édictées par les organismes d'assurance. Elle évalue les impacts probables des changements dans l'environnement légal et réglementaire.

Dans ce cadre, la fonction de « vérification de la conformité » doit identifier, évaluer et contrôler l'exposition aux risques légaux, juridiques et réglementaires. Enfin, elle apporte un conseil aux organes de gouvernance sur les problématiques de conformité. Ses missions se traduisent dans un plan de conformité déterminé en fonction des activités présentant un risque de non-conformité. La définition de ce plan s'inscrit dans l'animation du dispositif de contrôle interne des organismes d'assurance. Ce dernier permet aux organismes d'assurance de renforcer la conduite des activités par des moyens de contrôles (organisations, indicateurs, procédures, etc.) lui permettant de maîtriser ses risques ou de prévenir les zones de défaillance.

#### 2.1.2.4 Les autres fonctions support

Outre les fonctions prévues dans la directive *Solvabilité II*, d'autres fonctions participent à la deuxième ligne de défense, telles que le contrôle interne, la sécurité des systèmes (Responsabilité

[1] *CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Supervisory Reporting and Public Disclosure Requirements – (former Consultation Paper 58).*



© IFACI

Sécurité et Système d'Information) ou la continuité des activités, elles complètent l'action des directions support plus traditionnelles (directions financières, informatiques, ressources humaines, juridique, qualité, etc.) amenées à émettre des politiques et/ou directives applicables au sein des organisations.

*Les services fonctionnels, responsables de domaines d'expertise*

Les services fonctionnels jouent un rôle particulier, parfois considérable, dans le dispositif de contrôle interne,

- soit du fait qu'ils ont reçu une autorité et un pouvoir de contrôle sur certaines opérations ou certains processus,
- soit du fait de l'assistance effective, sur le terrain, qu'ils sont en mesure d'apporter aux différentes entités pour identifier, comprendre, évaluer les principaux risques afférents à leur domaine, et les aider à concevoir les contrôles techniques les plus pertinents.

Les missions des services fonctionnels sont souvent analysées en quatre grandes familles :

- missions opérationnelles : il convient d'assurer des activités opérationnelles, dans l'intérêt de l'ensemble du groupe. Exemples : produire les comptes consolidés, réaliser une augmentation de capital, effectuer les achats d'énergie ou de matières premières pour toutes les filiales, etc. ;
- missions normatives et régaliennes : proposer les politiques du groupe, par domaines d'activité, ainsi que les analyses de risque correspondantes et les meilleures procédures de contrôle obligatoires ou recommandées, développer les meilleures pratiques et les échanges, « *benchmarker* » en externe et en interne ;
- missions de conseil et d'assistance : offrir ses services aux unités qui en ont besoin, pour mettre en place certaines procédures, tableaux de bord ou autres systèmes ;
- missions de supervision : cette 4ème grande famille de missions qui consiste à observer et à rendre compte du fonctionnement effectif des processus dont ils ont la charge dans les diverses unités de l'entreprise ou du groupe, s'est considérablement développée depuis quelques années avec l'affirmation d'un fort degré de responsabilité des services fonctionnels sur les résultats et les performances des processus.

*Extrait de la prise de position de l'IFACI sur l'Urbanisme du contrôle interne, octobre 2008.*

### 2.1.3 L'audit interne

Enfin, la 3ème ligne de défense est constituée de la fonction audit interne qui est exercée d'une manière objective et indépendante des autres fonctions. Par son rattachement au plus haut niveau et la réalisation d'un plan d'audit fondé sur une approche par les risques, l'audit interne évalue

© IFACI

notamment l'adéquation et l'efficacité du système de contrôle interne et les autres éléments du système de gouvernance en conformité avec l'article 47 de la directive *Solvabilité II*. Les autres éléments à prendre en considération par l'audit interne peuvent concerner le fonctionnement des organes délibérants et exécutifs, les exigences de compétence et d'honorabilité, le processus d'évaluation interne du risque et de la solvabilité (ORSA), la maîtrise de la sous-traitance, etc.

L'exploitation des constats et des recommandations de l'audit interne permet d'enrichir la cartographie des risques et de la faire vivre.

L'audit interne rend compte de son évaluation du niveau de maîtrise des risques aux organes d'administration, de gestion ou de contrôle.

Les services d'audit exercent leurs missions conformément au cadre de référence international de l'IIA / IFACI.

### 2.1.4 En synthèse : six étapes clés et des responsabilités clairement définies

L'outil de cartographie des risques permet aux différents acteurs d'avoir une vision systématisée et régulièrement mise à jour des risques de l'organisme d'assurance. Si les managers prennent les risques et les endossent, les 2ème et 3ème lignes sont plus directement impliquées pour donner une assurance sur la maîtrise des risques et mettre à jour de la cartographie des risques.

| Principales étapes de la cartographie | Première ligne | Deuxième ligne | Troisième ligne | Parties du cahier de la recherche |
|---|---|---|---|---|
| **Identifier et évaluer les risques** | ☑ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☑ Utilisateur | ☐ Sponsor<br>☑ Coordinateur<br>☑ Contributeur<br>☑ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☑ Utilisateur | Partie 3.1<br>Partie 3.2<br>Partie 3.3 |
| **Définir des dispositifs de traitement des risques** | ☑ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☑ Utilisateur | ☐ Sponsor<br>☑ Coordinateur<br>☑ Contributeur<br>☑ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | Partie 3.3.3.2<br>Partie 3.1 |
| **Mettre en œuvre les traitements des risques** | ☑ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | ☐ Sponsor<br>☑ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☐ Contributeur<br>☐ Utilisateur | Partie 3.1<br>Partie 3.3.3.3 |
| **Assurer une surveillance permanente et le pilotage du niveau des risques résiduels** | ☑ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | ☐ Sponsor<br>☑ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☐ Contributeur<br>☑ Utilisateur | Partie 4 |



© IFACI

| Principales étapes de la cartographie | Première ligne | Deuxième ligne | Troisième ligne | Parties du cahier de la recherche |
|---|---|---|---|---|
| **Evaluer périodiquement le dispositif de gestion des risques** | ☐ Sponsor<br>☐ Coordinateur<br>☐ Contributeur<br>☑ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☐ Contributeur<br>☑ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | Partie 4.2.1.3 |
| **Mettre à jour la cartographie des risques** | ☑ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | ☐ Sponsor<br>☑ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | ☐ Sponsor<br>☐ Coordinateur<br>☑ Contributeur<br>☐ Utilisateur | Partie 3 |

## 2.2 Les instances de gouvernance

La gestion des risques est guidée et surveillée par les différents acteurs des organes d'administration, de gestion, ou de contrôle (ou AMSB - *Admistrative, Management or Supervisory Body* - en référence à la directive *Solvabilité II*) ainsi que par les membres de comité d'audit ou des risques, qui forment « le gouvernement d'entreprise ».

### 2.2.1 Organe d'administration, de gestion ou de contrôle

Il détermine les orientations stratégiques de l'organisme et crée l'environnement et les structures pour une gestion des risques efficace. Ses responsabilités portent, à la fois, sur la surveillance et le pilotage du système de gestion des risques. Il impacte les démarches de cartographies des risques à travers :

- La définition de la stratégie et de la politique des risques (notamment l'appétit pour les risques et les seuils de tolérance).
- L'approbation annuelle des politiques écrites concernant leur gestion des risques, leur contrôle interne, leur audit interne et, le cas échéant, la sous-traitance (article 41 de la directive *Solvabilité II*). Les politiques de gestion des risques concernent notamment les domaines cités à l'article 44 : la souscription et le provisionnement, la gestion actif-passif, les investissements, la gestion du risque de liquidité et de concentration, la gestion du risque opérationnel, la réassurance et les autres techniques d'atténuation du risque (annexe 7).
- Le suivi de l'adéquation des dispositifs de gestion des risques et du respect du niveau général des risques définis par l'organisme.

Il doit disposer des compétences et des ressources pour exercer ses missions. En outre, l'exercice de ses missions peut être réalisé au travers de comités spécialisés.

© IFACI

« En France, l'organe d'administration de gestion ou de contrôle sera représenté par le conseil d'administration et le directeur général ou, dans le cas d'une structure duale, par le conseil de surveillance et le directoire ».

*Rapport d'activité annuel 2012 de l'ACP*

Bien que la gestion des risques relève de la responsabilité collective de l'organe d'administration, de gestion ou de contrôle, celui-ci doit désigner au moins un membre pour surveiller l'efficacité du système de gestion des risques en place .

### 2.2.2 Gouvernance institutionnelle : comité d'audit et/ou des risques

Le comité d'audit (et/ou des risques) est une émanation du conseil, il joue un rôle essentiel dans le suivi de la qualité des dispositifs de gestion des risques et de contrôle interne des organismes d'assurance et bénéficie à ce titre de *reporting* s'appuyant parfois sur des cartographies des risques, dont les travaux d'audit interne.

Il apprécie toute déviance par rapport au cadre de tolérance aux risques, défini par l'organe d'administration, de gestion ou de contrôle, sur la base notamment d'études prospectives et de différents exposés techniques.

Le comité d'audit doit disposer de plusieurs sources d'information (cartographie des risques, synthèse des CAC, rapports d'audit interne, etc.) et veiller à la cohérence globale de ces documents. Le comité d'audit avec la mise en œuvre de la directive *Solvabilité II* devra émettre des avis sur plusieurs politiques et rapports (dont le rapport ORSA et le rapport actuariel qui comprend un avis sur la politique de souscription et les provisions).

### 2.2.3 Gouvernance opérationnelle : comité managérial des risques

Le comité des risques visé ici est un comité managérial interne dont le positionnement et le rôle sont tout à fait différents de ceux du comité d'audit et/ou des risques évoqués ci-dessus. Sa présidence est assurée par un membre de l'organe dirigeant et il est dédié à la surveillance et au pilotage de la solvabilité ainsi qu'au management de l'ensemble des risques significatifs et élevés :

- les risques visés dans la formule standard (souscription, marché, opérationnel, etc.),
- les autres risques non ou mal appréhendés dans la formule standard : risques stratégiques, de pilotage et d'image.



© IFACI

Sur proposition de la direction des risques, le comité prend les principales décisions concernant la mise en œuvre des dispositifs de gestion des risques et l'encadrement des principaux risques. Il assure le suivi de la mise en œuvre des solutions de remédiation.

### 2.2.4 Autres comités internes participant à la gestion des risques dans le cadre de décisions opérationnelles

Pour assurer le déploiement opérationnel de la gestion des risques, les organismes d'assurance mettent en place des comités managériaux tels que :

- le comité de gestion actif-passif (ALM - *Asset and Liability Management*)
- le comité de souscription,
- le comité des placements,
- etc.

Ces comités managériaux doivent être transverses. Les informations et les décisions doivent circuler de manière très fluide entre les structures.

La gouvernance des comités doit être formalisée par un règlement intérieur (composition, mode de fonctionnement, périmètre, création éventuelle de sous-comités, dispositif de remontée d'information, etc.).

Tout comité doit émettre et archiver un ordre du jour, un compte rendu et les documents présentés en séance.

L'audit interne doit avoir accès à l'information, notamment pour l'élaboration du plan. Ainsi,l'audit interne doit être destinataire des comptes rendus des comités et/ou être invité aux comités, avec voix consultative.

© IFACI

© IFACI

# Partie 3

# Identification et évaluation des risques

Le recensement des risques vise à capter à un instant donné, les risques qui peuvent porter atteinte à la réalisation des objectifs d'une organisation, d'un processus, ou d'une activité.

© IFACI

## 3.1 La notion de risque

Les référentiels de contrôle interne et de gestion des risques proposés dans la partie 1 proposent des définitions et des principes pour mieux appréhender les risques.

### 3.1.1 Définitions

Selon la norme ISO 31000 qui fait référence au Guide 73:2009 « Management du risque – Vocabulaire », le risque est « l'effet de l'incertitude sur l'atteinte des objectifs ». A noter que cette définition ne caractérise pas l'effet, celui-ci peut donc être un écart négatif ou positif par rapport aux attentes.

Les objectifs en questions peuvent avoir différents aspects (par exemple, objectifs financiers, de conformité, opérationnels, etc.) et peuvent concerner différents niveaux (stratégique, projet, produit, processus ou un organisme tout entier).

Le cadre de référence de l'AMF considère que « le risque représente la possibilité qu'un événement survienne et dont les conséquences seraient susceptibles d'affecter les personnes, les actifs, l'environnement, les objectifs de la société ou sa réputation ».

Le COSO définit le risque comme étant « la possibilité qu'un événement se produise et affecte la réalisation des objectifs »[1]. « Dans le cadre du processus d'identification et d'évaluation des risques, une organisation peut également déceler des opportunités, qui sont des événements susceptibles d'affecter positivement la réalisation des objectifs. Il est important de saisir ces opportunités et de les communiquer au processus de définition des objectifs »[2].

Pour ses travaux, l'unité de recherche s'est basée sur la définition du risque proposée par le COSO en 2013.

Ces référentiels proposent d'appréhender les risques selon au moins deux dimensions : d'une part, par les notions de fréquence, de probabilité, d'aléas, d'incertitude, et d'autre part, par les conséquences, les impacts sur les organisations, les individus ou les objectifs. Seule la combinaison de ces deux composantes (par exemple, la fréquence et l'impact) permet d'estimer raisonnablement le niveau de risque.

Enfin, il convient de distinguer :

- **le risque brut** ou inhérent qui mesure le risque sans aucun élément de maîtrise : absence de procédures, absence d'activités de contrôle, absence de système informatique, etc.

[1] *Cf. Internal Control - Integrated Framework / COSO. - mai 2013. La version française paraîtra début 2014.*
[2] *Composante évaluation des risques du COSO 2013.*


© IFACI

- **le risque résiduel** ou le risque net qui mesure le risque après mise en place des éléments de maîtrise : contrôle interne, couverture financière, partage du risque, etc.

### 3.1.2 Appétence pour les risques et seuil de tolérance

L'appétence pour le risque est en général formulée de façon quantitative ou qualitative. Définie par les organes de gouvernance et de direction, elle encadre la prise de risque en fixant les limites des impacts qu'un organisme est prêt à accepter. Ce concept se traduit pratiquement dans la gestion quotidienne de l'entreprise : par exemple, les politiques de souscription cadrent les produits autorisés à la vente, ou les conditions de souscription acceptables, ou les engagements maximaux.

Elle est souvent complétée par la notion de tolérance au risque définit dans le COSO 2 comme « le niveau de variation acceptable dans l'atteinte d'un objectif ». Par exemple, si l'objectif de satisfaction des clients est fixé à 98%, l'organisation peut accepter une tolérance de 96 à 100%.

La mise en œuvre opérationnelle de ces critères nécessite donc une identification préalable des objectifs et des conséquences des risques. Ils permettent de retenir les mesures de traitement appropriées pour maintenir les niveaux de risque en deçà de ces seuils. Ils sont donc utilisés dans le cadre du contrôle interne pour la conception et le suivi de l'efficacité des éléments de maîtrise.

*Conception et suivi des indicateurs de risques*

Des indicateurs de risques et des seuils d'alerte sont conçus et suivis à chaque niveau du dispositif :

- Au niveau des instances de gouvernance, c'est essentiellement l'appétence globale pour les risques qui est déterminée en fonction de la stratégie et des valeurs de l'organisation. L'organe dirigeant fixe les objectifs généraux en précisant une tolérance de déviation et un horizon temporel. La direction générale s'assure de la bonne déclinaison de ces métriques dans les différentes activités.
- Les fonctions en charge du suivi des risques proposent, en lien avec les directions métiers concernées, des indicateurs permettant de vérifier l'adéquation des données remontées des directions opérationnelles par rapport au profil de risque défini (appétence et tolérance définies par les instances de gouvernance). Pour ce faire, elles peuvent être amenées à accompagner la spécification de ces limites et la mise en œuvre des éléments de maîtrise des risques avec les directions métiers. Elles rendent comptent, en autonomie par rapport aux directions opérationnelles, aux instances de gouvernance, le cas échéant, elles accompagnent la mise en œuvre des actions correctrices.
- Les directions opérationnelles s'approprient les métriques de la politique de risques. Pour cette déclinaison et pour la maîtrise de leurs activités, elles peuvent s'appuyer sur les fonctions de la deuxième ligne de défense, et en particulier les directions de la gestion des risques, du contrôle interne ou de la conformité.

© IFACI

- L'audit interne vérifie de façon indépendante que la politique des risques est clairement définie pour être mise en œuvre par la première et la deuxième ligne de défense. Il s'assure périodiquement que le niveau de maîtrise des processus reste dans les limites acceptables. Il fait des propositions pour améliorer la gestion globale du dispositif et la fiabilité des indicateurs.

*Bonne pratique concernant les indicateurs de risques :*

Les indicateurs conçus et utilisés aux différents niveaux du dispositif doivent être cohérents les uns avec les autres.
Les indicateurs doivent être directement liés aux limites de risque définies. Ils constituent le lien entre la réalité opérationnelle et le pilotage de l'entreprise.
Ils doivent être compréhensibles par des non techniciens et permettre la prise de décision.
Des alertes doivent être mise en place sur ces indicateurs pour vérifier que les limites ne sont pas dépassées.

### 3.1.3 La nomenclature des risques

La typologie des risques proposée par l'unité de recherche facilite :

- l'identification des risques,
- la bonne couverture du recensement des risques,
- l'établissement de liens entre les risques captés à des niveaux différents,
- le dialogue entre les différents acteurs,
- la consolidation des différents *reporting* opérationnels ou réglementaires.

Deux principales natures de risques sont rencontrées (cf. également le modèle FERMA dans la partie 1.2) :

- les risques endogènes, propres à l'activité de l'organisation, qui sont liés à ses processus, son organisation, son système d'information, son management, etc.
- les risques exogènes dont l'origine provient de l'environnement de l'organisation : les clients, les fournisseurs, les sociétaires ou actionnaires, les concurrents, les marchés financiers, les catastrophes naturelles ; l'organisation ayant peu d'emprise sur cette nature de risques, il est néanmoins nécessaire de mettre des éléments de maîtrise et de surveillance pour en limiter les impacts.


© IFACI

### 3.1.3.1 Une classification en 4 grandes familles

Conçu de manière arborescente selon trois niveaux de risques, la nomenclature de l'unité de recherche proposée en annexe 2 permet de préciser les risques identifiés et de les rattacher à l'une des quatre familles de risques retenues[1].

Cette nomenclature est construite sur trois niveaux de risques complémentaires :

- le **niveau 1** concerne les quatre grandes familles de risques :
  - **financiers :** risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière ;
  - **assurances :** risques spécifiques aux activités techniques d'assurance (souscription, tarification, provisionnement technique, etc.) ;
  - **opérationnels :** risques de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs ;
  - **stratégiques et environnementaux :** risques relatifs au pilotage de l'entreprise, aux risques de réputation directs et aux risques générés par l'environnement de l'entreprise et aux risques émergents.
- le **niveau 2** permet de définir des catégories de risques au sein de chaque famille (exemple pour les risques financiers : liquidité, marché, crédit, etc.).
- le **niveau 3** offre un degré de détail supplémentaire au sein de ces catégories (exemple : pour le risque financier de crédit : règlement livraison, défaut émetteur, etc.).

Chacune de ces quatre familles a été déclinée en 27 risques de niveau 2, lesquels ont été à leur tour déclinés en 192 risques de niveau 3. Ainsi, selon le niveau de granularité souhaité, elle permet d'avoir un degré de finesse variable dans la vision des risques encourus.

De plus, cette nomenclature actualisée intègre les risques définis pour la formule standard par la directive *Solvabilité II*.

### 3.1.3.2 Focus sur le risque opérationnel

L'article 13 de la directive *Solvabilité II* (cf. annexe 7), définit le risque opérationnel comme le « risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs». Cette définition englobe une grande diversité de risques. Hormis, la mention aux événements externes, elle est très proche de celle proposée par Bâle 2 qui vise les pertes directes ou indirectes dues à une inadéquation ou à une défaillance des procédures, du personnel et des systèmes internes. Compte tenu de cette similitude, l'unité de recherche a repris la déclinaison en sept catégories du risque opérationnel de Bâle 2 :

- clients, produits et pratiques commerciales,
- exécution, livraison et gestion des processus,

[1] *Le précédent référentiel comportait 6 familles de risques (assurance, financier, comptable, opérationnel, pilotage, externe), ce passage à 4 familles de risques s'explique par le retour d'expérience des membres de l'unité de recherche – Cf. Cartographie des risques / Groupe professionnel « Assurance ». – IFACI, 2006.*

© IFACI

- dysfonctionnements de l'activité et des systèmes,
- pratiques en matière d'emploi et de sécurité sur le lieu de travail,
- dommages aux actifs corporels,
- fraude interne,
- fraude externe.

En vertu de l'article 49.2.b de la directive *Solvabilité II*, la sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques ne doit pas être effectuée d'une manière susceptible d'accroître indûment le risque opérationnel. Pour maîtriser les risques opérationnels, il est donc indispensable de ne pas se limiter aux frontières de l'organisation. Pour mémoire, un groupe de recherche de l'IFACI a fait des propositions pour la maîtrise des activités en délégation de gestion[1].

Compte tenu de la palette des risques opérationnels, il n'est pas rare de trouver des cartographies thématiques, par exemple, sur le risque de fraude ou les pratiques commerciales.

### 3.1.3.3 *Focus sur les risques de la formule standard sous* Solvabilité II

Sous le régime *Solvabilité II*, le SCR[2] (capital de solvabilité requis) représente l'exigence de capital. Il correspond au montant de fonds propres à détenir pour permettre d'éviter la ruine à 99,5 % à l'horizon d'un an.

Le SCR est basé sur le profil de risque de l'organisme d'assurance, le SCR peut être calculé soit par une formule standard calibrée uniformément sur le marché européen, soit par un modèle interne développé par l'organisme d'assurance et après autorisation par le superviseur, soit par une combinaison de ces deux méthodes.

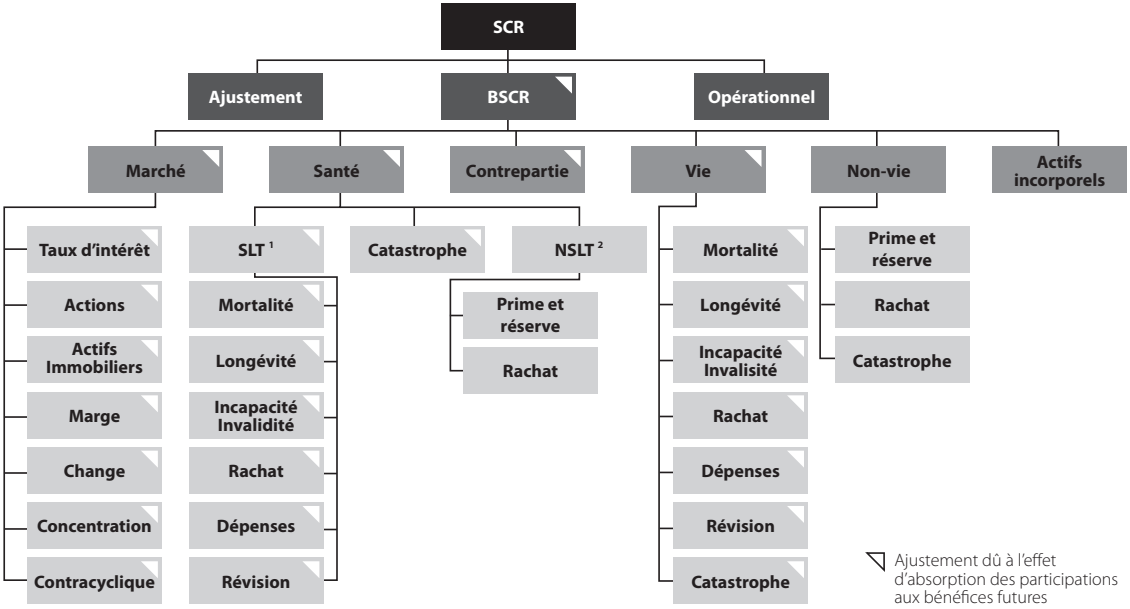
Le SCR « formule standard » est calculé selon une approche modulaire (cf. schéma ci-après). L'organisme doit calculer la perte subie en cas d'événement défavorable lié à une trentaine de sous-modules de risques, répartie à travers sept modules de risques[3] :

- Le module « risque de marché »,
- Le module « risque de souscription en santé »,
- Le module « risque de contrepartie »,
- Le module « risque de souscription en vie »,
- Le module « risque de souscription en non-vie »,
- Le module « risque sur actifs incorporels »,
- Le risque opérationnel.

[1] *La délégation de gestion en assurances de personnes : pistes pour un contrôle interne efficace [Cahier de la Recherche] / Unité de Recherche de l'IFACI. - IFACI, 2012.*
[2] *Solvency Capital Requirement.*
[3] *Cf. Annexe 3 : Présentation des risques de la formule standard.*


© IFACI

Les risques décrits pour déterminer la formule standard constituent donc une base pour cartographier les risques de l'organisme d'assurance. Aussi, la nomenclature des risques présentée en annexe 2, fait référence aux modules et sous modules de risques de cette formule.




[1] SLT (*Similar to Life insurance Techniques)* : Similaire aux techniques d'assurance-vie
[2] NSLT (*Non Similar to Life insurance Techniques)* : Non similaire aux techniques d'assurance-vie

*D'après le schéma de la directive Solvabilité II.*

## 3.2 Mesure du risque

A minima, deux critères sont appréciés pour coter le **risque brut** : la fréquence et l'impact :

*Risque brut = Fréquence x Impact*

Le **risque résiduel** mesure le risque après mise en place des éléments de maîtrise :

*Risque résiduel = Fréquence x Impact x Elément de maîtrise*

Les échelles d'évaluation facilitent la hiérarchisation des risques et *in fine* les arbitrages sur des actions à mener. Les échelles paires à quatre niveaux sont à privilégier.

© IFACI

### 3.2.1 La fréquence

Comment déterminer la fréquence de survenance du risque ? Par l'estimation de l'occurrence des événements pouvant être à l'origine du risque. L'échelle de mesure de la fréquence doit être établie et adaptée à la structure.

Ci-après sont proposées deux illustrations de mesure de la fréquence.

*Illustration 1 : Echelle de mesure de la fréquence*

| Cotation | Fréquence | Elément de mesure |
|---|---|---|
| **1** | Exceptionnel | Occurrence quasi nulle (<1%) sur 2 ans |
| **2** | Rare | Occurrence possible mais peu probable (1 à 10%) sur 2 ans |
| **3** | Probable | Occurrence plausible (10 à 50%) sur 2 ans |
| **4** | Très probable | Occurrence très probable (>50%) sur 2 ans |

*Illustration 2 : Echelle de mesure de la fréquence*

| Cotation | Fréquence | Elément de mesure |
|---|---|---|
| **1** | Rare | Fréquence de l'ordre d'1 à 2 fois en 3 ans |
| **2** | Modéré | Fréquence de l'ordre d'1 fois par an |
| **3** | Occasionnel | Fréquence pluriannuelle (quelques fois par an, de l'ordre du trimestre, du mois) |
| **4** | Fréquent | Fréquence quotidienne ou hebdomadaire |



© IFACI

*Illustration 3 : Probabilité d'occurrence - Menaces*

| Estimation | Description | Indicateurs |
|---|---|---|
| Forte (probable) | Susceptible de survenir chaque année ou plus de 25% de chances de survenir. | A le potentiel de survenir plusieurs fois dans la période considérée (par exemple dix ans).<br>S'est produit récemment. |
| Modérée (possible) | Susceptible de survenir dans les dix prochaines années ou moins de 25% de chances de survenir. | Pourrait survenir plus d'une fois dans la période considérée (par exemple dix ans).<br>Peut être difficile à maîtriser en raison d'influences externes.<br>Y a-t-il un historique de survenance ? |
| Faible (peu probable) | Peu susceptible de survenir dans les dix prochaines années ou moins de 2% de chances de survenir. | Ne s'est pas encore produit.<br>Peu susceptible de survenir. |

*Source : Cadre de référence de la Gestion des Risques / FERMA. – 2003.*

## 3.2.2 L'impact

Quelle est la conséquence si le risque se concrétise ? L'unité de recherche propose de décliner les impacts en 3 principales catégories[1], à savoir :

- l'impact financier (ex : perte financière, baisse des revenus, hausse des coûts), direct ou indirect, immédiat ou à terme. L'annexe 4 vous propose une liste non-exhaustive d'impacts financiers ;
- l'impact juridique (ex : responsabilité civile et/ou pénale, sanctions légales et/ou professionnelles, etc.) ;
- l'impact sur l'image (dégradation de l'image, réputation remise en cause).

Une estimation systématique des conséquences financières, basée sur des scénarios de risques précis peut être un exercice très lourd et complexe. Il est en effet difficile d'exiger une évaluation financière précise de tous les impacts (humains, conformité, réputation, etc.).

Pour faciliter l'exercice d'évaluation, il est toutefois souhaitable d'établir des critères objectifs pour chaque niveau de gravité.

[1] *Ces trois principales catégories d'impact sont adaptées au secteur assurantiel. En fonction du domaine d'activité des entreprises, d'autres catégories d'impact peuvent être pertinentes. Par exemple, les impacts environnementaux peuvent être appropriés à l'industrie (nucléaire, minière, pétrolière) ou encore les impacts sur la vie humaine peuvent être envisagés dans les secteurs des travaux publics, de la sécurité (armée, police), ou l'industrie minière.*

© IFACI

L'échelle de mesure de l'impact doit être établie et adaptée à l'organisme. Ci-après sont proposées deux illustrations de mesure de l'impact. D'autres évaluations de l'impact financier sont proposées en annexe 4.

*Illustration 1 : Echelle de mesure de l'impact*

| Impact | | Impact financier | Impact image | Impact légal réglementaire |
|---|---|---|---|---|
| 1 | Faible | < 10 000 euros | Impact local | Observation des autorités de tutelle |
| 2 | Modéré | Entre 10 000 à 100 000 euros | Impact régional | Avertissement des autorités de tutelle<br>Mise en cause juridique devant une juridiction autre que pénale |
| 3 | Significatif | Entre 100 000 à 500 000 euros | Impact national<br>Un seul canal | Blâme des autorités de tutelle<br>Mise en cause devant une juridiction pénale |
| 4 | Elevé | > 500 000 euros | Impact national<br>Couverture large | Sanction des autorités de tutelles<br>Condamnation pénale |

*Illustration 2 : Echelle de mesure de l'impact*

| Cotation | Impact | Financier (Résultat) | Image / réputation ou encore réglementaire |
|---|---|---|---|
| 1 | Limité | < 10% du résultat annuel | Attention de tiers (presse, groupes de pression, etc.) sur des sujets jugés sensibles |
| 2 | Significatif | 10% à 50% du résultat annuel | Communication défavorable dans des médias sur une partie de l'entreprise et à un niveau local |
| 3 | Majeur | 50% à 100% | Couverture médiatique plus large, mais n'entraînant pas d'effet majeur |
| 4 | Critique | > au résultat annuel | Attaque médiatique ayant des conséquences significatives sur l'image et la réputation du Groupe |

### *Comment définir les seuils financiers dans les échelles de mesure d'impact ?*

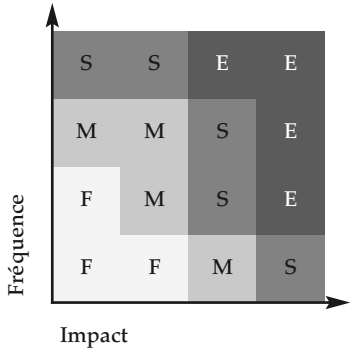
Les différents seuils à retenir doivent être « discriminants » et permettre une distribution des risques régulière sur l'ensemble des seuils retenus : si tous les risques évalués se situent sur le même niveau, l'échelle retenue ne sera pas utile à la bonne hiérarchisation des risques.



© IFACI

## 3.2.3 Le risque brut

L'impact et la fréquence permettent de déterminer la cotation brute ou inhérente du risque.




| | |
|---|---|
| F | Risque Faible |
| M | Risque Modéré |
| S | Risque Significatif |
| E | Risque Elevé |

Pour certains, cette étape est considérée comme une étape intermédiaire. Ils préfèrent directement raisonner sur le risque résiduel, en intégrant les éléments de maîtrise dès les premiers travaux d'évaluation des risques. Ils résolvent ainsi une limite cognitive des acteurs qui n'arrivent pas à raisonner sur les risques en faisant abstraction des éléments de maîtrise existants.

## 3.2.4 Les éléments de maîtrise

L'élément de maîtrise se définit comme le moyen existant ou à mettre en place pour permettre de réduire ou d'éliminer le risque. Il peut porter aussi bien sur la fréquence que sur l'impact du risque à titre préventif ou correctif. Ainsi, à chaque risque est associé un ou plusieurs éléments de maîtrise. Il est entendu qu'un même élément de maîtrise peut venir agir sur plusieurs risques.

Ces éléments de maîtrise sont constitués généralement de :

- missions, tâches données aux collaborateurs,
- manuels de procédures, modes opératoires,
- niveaux de savoir-faire des collaborateurs,
- tableaux de bord,
- systèmes informatiques,
- organigrammes ou structures clairement définis et formalisés,
- directives, consignes, règles claires et écrites,
- actions de vérifications : auto-contrôle, contrôle humain, contrôle automatique,
- séparation des tâches,
- délégations de pouvoirs formalisées.

L'échelle d'appréciation des éléments de maîtrise doit être établie et adaptée à l'organisme.

© IFACI

*Illustration 1 : Echelle d'appréciation des éléments de maîtrise*

| Cotation | Niveau de maîtrise | Elément de mesure |
|---|---|---|
| 1 | Maitrisé | Dispositifs mis en place permettant de réduire la fréquence ou l'impact du risque à un niveau satisfaisant : règles écrites et détaillées, contrôles formalisés et appliqués (indicateurs de suivi et de contrôle, évaluation des procédures, etc.). |
| 2 | Acceptable | Dispositifs mis en place permettant de réduire notablement la fréquence ou l'impact du risque : règles écrites mais à compléter, éléments de maîtrise existants et pertinents, formalisés mais à compléter. |
| 3 | Insuffisant | Dispositifs mis en place ne permettant pas de réduire significativement la fréquence ou l'impact du risque : règles orales, éléments de maîtrise partiellement existants ou pertinents et peu formalisés. |
| 4 | Faible | Absence d'élément de maîtrise : pas ou peu de règle, on se fie à l'expérience, pas ou peu de remontées d'informations, pas ou peu de sensibilisation du personnel aux risques. |

## 3.2.5 Le risque résiduel

Le risque résiduel est la criticité que présente le risque après prise en compte de l'effet protecteur des éléments de maîtrise en place.

*Risque résiduel = Fréquence x Impact x Elément de maîtrise*

Le poids du risque ainsi déterminé permet une hiérarchisation des principaux risques et une priorisation des plans d'actions peut être établie.

***Illustration 1 : Echelle de mesure du risque résiduel***

| | |
|---|---|
| **L = risque faible**, géré par les procédures en place | L'impact sur l'atteinte des objectifs n'est pas préoccupant, le risque est sous contrôle |
| **M = risque modére**, un suivi spécifique doit être organisé | L'impact sur l'atteinte des objectifs est limité. Des actions doivent être entreprises mais ne sont pas urgentes. |
| **S = risque significatif**, une alerte au senior management est nécessaire | L'impact sur l'atteinte des objectifs est significatif. Nécessité de prendre des actions immédiates pour limiter le risque. |
| **H = risque élevé**, action immédiate requise | L'impact sur l'atteinte des objectifs est d'une telle ampleur que les objectifs ne seront très probablement pas atteints. Nécessité de prendre des actions immédiates pour limiter le risque, et alerter la direction. |



© IFACI

Les risk managers peuvent mobiliser des critères complémentaires à l'impact et à la fréquence pour affiner l'évaluation des risques. Par exemple :

- la vélocité,
- la volatilité,
- le fait qu'il soit plus ou moins contrôlable,
- la capacité.

## 3.3 Deux approches complémentaires

Du fait des évolutions rapides de l'environnement règlementaire et de la complexification des activités, les directions générales ont fait de la cartographie des risques un véritable outil global de pilotage et en sont devenues les principaux commanditaires.

L'appréhension systématique des risques se fait généralement selon deux approches :

- **L'approche** ***bottom-up,*** partant de l'analyse des processus et permettant de mettre en œuvre les dispositifs de maîtrise des risques adéquats.
- **L'approche** ***top-down,*** partant de la vision du top management et permettant d'aboutir directement à une évaluation des expositions majeures pour l'organisation.

Le rapprochement entre ces deux approches doit permettre à l'organisme d'assurance d'identifier les risques pouvant avoir un impact sur les objectifs majeurs de l'organisation et d'aboutir à une cartographie globale des risques pour un pilotage efficace de l'organisation.

### 3.3.1 L'approche *bottom-up*

L'approche *bottom-up* (ou l'approche par les processus) d'identification et d'évaluation des risques repose sur les étapes suivantes :

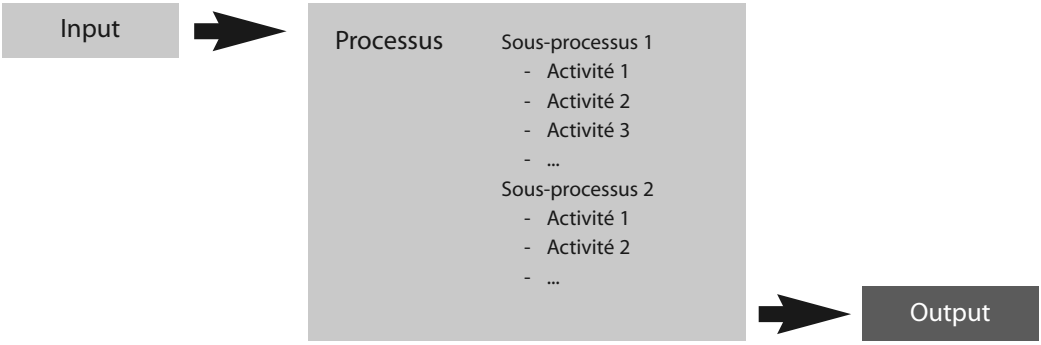
1. Identification des processus.
2. Identification et cotation des risques au niveau de chaque processus.
3. Identification et évaluation des éléments de maîtrise existants.
4. Cotation du risque résiduel.

#### *3.3.1.1 Identification des processus*

Un processus peut être défini comme l'ensemble des opérations ou activités réalisées par des

© IFACI

acteurs, avec des moyens et dans un cadre donné, à partir d'un événement déclencheur externe *(input)* pour aboutir à un résultat, une finalité *(ouput)*.




Partir des processus permet de s'appuyer sur un cadre plus stable que les structures organisationnelles.

Le recensement des processus de l'entreprise est fonction du modèle économique et est généralement réalisé par (ou en liaison avec) la direction de l'organisation ou de la qualité.

Pour les organismes d'assurance ayant déjà décrit les processus dans le cadre de démarches connexes telles que la certification ISO ou encore de formalisation des procédures de l'entreprise, il est recommandé de s'appuyer sur les démarches existantes afin d'une part d'optimiser les moyens et d'autre part assurer une homogénéité des démarches dans les organisations.

Les processus peuvent être classés en 2 grandes familles :

- les processus relatifs à la production quotidienne **(processus métiers ou opérationnel)**,
- les processus relatifs au bon fonctionnement **(processus supports)**.

L'annexe 1 propose une illustration des principaux processus d'un organisme d'assurance.

Le niveau de granularité retenu dépendra des objectifs de la cartographie et de la taille des organisations. Ce niveau doit être suffisamment fin pour identifier de façon pertinente les risques significatifs mais ne doit pas conduire à lister l'ensemble des tâches de l'organisation.

La définition de la granularité est essentielle car plus le niveau de détail est fin, et plus le travail correspondant d'identification des risques est important. Elle impacte donc l'élaboration de la cartographie et sa maintenance ultérieure.



© IFACI

Choisir le bon niveau de granularité est également important afin de calibrer la démarche aux moyens disponibles et au planning souhaité. Ainsi, cinq niveaux de granularité, en partant du plus large au plus particulier, sont proposés :

- **le métier :** IARD, vie, assistance, réassurance, etc. ;
- **le domaine :** pour le métier IARD : habitat, auto, transport aérien, etc. ;
- **le processus :** processus de souscription, processus de paiement des prestations, etc. ;
- **l'activité :** pour le processus de paiement des prestations : enregistrement, règlement du sinistre, etc. ;
- **la tâche élémentaire :** pour l'opération règlement du sinistre : envoi du chèque.

C'est la granularité qui déterminera le niveau hiérarchique adéquat des interlocuteurs à rencontrer afin de collecter les informations.

L'unité de recherche s'est accordée pour désigner le niveau médian « processus » comme le niveau pertinent d'une cartographie. En effet, celui-ci constitue d'une part le meilleur compromis entre le temps passé à l'élaboration de la cartographie et le degré de pertinence de la vision des risques. D'autre part, c'est le niveau d'équilibre permettant de faire converger et de relier les éléments obtenus selon les deux principales méthodes (*top-down* et *bottom-up*).

Il est possible de limiter le périmètre de la cartographie en ne retenant que des « processus clés ». Il s'agit, par exemple, des processus à impact client fort ou identifiés comme particulièrement exposés financièrement.

*Ecueils à éviter*

La maturité de l'organisme d'assurance en matière d'approche par les processus est un facteur clé de succès : à défaut de processus suffisamment précis et stabilisés, l'étape suivante d'identification des risques peut vite devenir complexe avec des redondances inutiles. Dans ce cas, une entrée supplémentaire par entités / directions peut être nécessaire.

#### 3.3.1.2 Identification et cotation des risques au niveau des processus

Une première identification des risques est réalisée au cours des entretiens ou d'ateliers avec les opérationnels. Comme pour le recensement des processus, la description des risques peut se faire soit sur la base d'un questionnaire soit de manière ouverte, facilitant ainsi l'identification des risques.

Cette première identification est construite conjointement par le management de l'activité opérationnelle et les équipes en charge de la cartographie des risques. Chaque risque est établi à partir de la collecte d'informations sur le domaine concerné, et le partage des enjeux et des probléma-

© IFACI

tiques avec le responsable du périmètre. Un risque doit faire l'objet d'une définition précise. Il en va de l'efficacité du dispositif de maîtrise qui découlera de la cartographie.

Pour ce faire, le risque est généralement documenté avec les caractéristiques suivantes :

- Le contexte dans lequel le risque s'inscrit (ex. : maîtrise de la sinistralité dans un environnement économique conjoncturel difficile et concurrentiel fort).
- La description du risque, (ex. : risque de paiement à tort d'une prestation, dans le processus de gestion des prestations).
- Les causes possibles du risque (ex. : absence de supervision).
- Eventuellement les facteurs de risques, à savoir les éléments aggravants (ex. : changement d'organisation récent).
- Les impacts ou les conséquences possibles (ex. : paiement d'une prestation à tort => impact financier : du montant de la prestation payée à tort). Sa fréquence, établie le plus souvent à dire d'expert, de retour d'expérience (ex. : probabilité de payer à tort représente 2% des dossiers traités).

Le recensement des risques étant réalisé à partir de différentes activités prises isolément, il est important d'identifier également les risques liés aux interrelations entre ces activités.

Boîte à outils : *Questions clés pour recenser les risques au niveau des processus*

La démarche consiste à identifier tout ce qui pourrait empêcher la réalisation des objectifs du processus. Il convient donc d'avoir, pour chaque processus, une vision claire des objectifs et des critères de performance attendus. Les informations recueillies lors de la description des processus permettent de répondre aux questions :

- Quels sont les objectifs du processus ?
- Quels sont les facteurs clés de succès ?
- Quels sont les critères de performance attendus du processus ?

| | |
|---|---|
| **Rechercher les risques liés aux éléments intrinsèques au processus** | • Quels dysfonctionnements sont susceptibles d'intervenir dans le déroulement du processus ?<br>• Quelles sont les phases critiques du processus : qu'est-ce qui pourrait échouer ?<br>• Qu'est-ce qui doit impérativement fonctionner correctement ?<br>• Quels sont les maillons faibles au sein du processus ?<br>• Quelles sont les ressources clés à protéger ?<br>• Quels sont les erreurs, omissions, actions ou incidents qui peuvent avoir un impact significatif sur la performance du processus ?<br>• Votre organisation est-elle adaptée à vos activités ? Préciser.<br>• Votre système d'informations est-il adapté à vos besoins ? Préciser. |



© IFACI

| | |
|---|---|
| **Identifier les risques provenant de facteurs externes au processus** | • En quoi les autres processus peuvent interférer négativement sur la performance du processus ?<br>• Quels sont les points de dépendance les plus critiques ? (systèmes d'information instables, qualité des informations reçues insuffisante, etc.)<br>• En quoi « l'environnement » actuel peut empêcher la réalisation des objectifs du processus ?<br>• En quoi une évolution de « l'environnement » peut empêcher la réalisation des objectifs du processus ?<br>• Quelles causes externes rendent le processus plus vulnérable : évolution de l'environnement légal ou réglementaire, de l'environnement concurrentiel, de l'environnement technologique, etc. |

- Chercher à avoir une vision exhaustive des risques même si le risque est faible pour pouvoir suivre son évolution.
- La documentation structurée de chaque risque est un investissement pour l'ensemble du dispositif. En effet, certains d'entre eux peuvent être repris pour établir une cartographie sur des périmètres analogues bien que distincts (même type d'activité, même nature de problématiques, etc.).

### *3.3.1.3 Identification et évaluation des éléments de maîtrise existants*

De même que lors de l'identification et de l'évaluation des risques, les éléments de maîtrise doivent être documentés et appréciés notamment à partir de données sur :

- l'organisation (par exemple, pour répondre à la question de l'organisation de la gestion des prestations ; collecter les éléments relatifs à l'organisation, aux définitions de postes, aux habilitations ouvertes dans les SI, aux règles de séparation de fonction) ;
- le management et l'animation ;
- la documentation (ex. : existence de procédure et modes opératoires relatives à la gestion des prestations) ;
- la formation (ex. : existence de formations régulières et actualisées) ;
- les activités de contrôle (quels types de contrôles [humain, automatique] ? Par exemple, contrôles manuels, vérification par une tierce personne, en fonction de la nature et le montant de la prestation, avant paiement de la prestation) ;
- le *reporting* et le suivi d'activité (ex. : nombre de dossiers traités et montant payé, analyse des écarts éventuels d'une période sur l'autre).

Cette analyse pourra se fonder sur des constats factuels de la réalité de l'existence et de l'efficacité des éléments de maîtrise.

© IFACI

#### 3.3.1.4 Cotation du risque résiduel

Une fois les éléments relatifs aux risques et aux éléments de maîtrise identifiés, la cotation du risque résiduel peut être obtenue.

*Risque résiduel = Fréquence x Impact x Elément de maitrise*

*Exemple : Risque de paiement à tort associé au processus de gestion des prestations.*

A partir des métriques présentées (Parties 3.2.1 / 3.2.2 / 3.2.4 / 3.2.5 - Illustrations 1).
Pour le règlement d'un capital décès (200 000 €).
La fréquence de payer à tort est estimée comme occasionnelle => cotation = 3.
L'impact de 200 000 € considéré comme significatif => cotation = 3.
Les éléments de maîtrise sont faibles : pas de procédure formalisée, pas de contrôle de supervision pour les sinistres lourds, calcul des garanties et du montant de la prestation non intégré dans le SI => cotation = 4.
Risque résiduel = 3x3x4 = 36, qui présente un risque élevé et nécessite la mise en place d'actions correctives et de mesures de maîtrise des risques.

*Les cartographies thématiques*

Il existe de plus en plus de cartographies des risques thématiques pour le diagnostic de sujets particuliers. Les plus courantes sont les cartographies des risques liés aux systèmes d'information, aux risques juridiques, aux risques de blanchiment des capitaux et du financement du terrorisme ou encore aux risques de fraude. Les méthodes utilisées sont similaires à celles exposées ci-dessus mais elles peuvent s'enrichir de critères spécifiques pour l'évaluation des risques (par exemple, temps d'indisponibilité pour les systèmes d'information).

### 3.3.2 L'approche *top-down*

La cartographie des risques *top-down* est une démarche qui consiste à collecter au niveau du top management, l'ensemble des grands risques pouvant limiter ou **empêcher l'atteinte des objectifs stratégiques de l'organisation, ou menacer ses principaux actifs. Elle se déroule selon** les étapes suivantes :

1. L'identification des risques et leur évaluation.
2. Le rapprochement de ces risques avec la nomenclature des risques de l'organisation.
3. Le rapprochement de ces risques avec les processus de l'organisation.



© IFACI

#### *3.3.2.1 Identification et évaluation des risques à dire d'expert*

Le top management est en mesure de recenser les grands risques avec un impact fort ou/et une fréquence importante. Ce type d'analyse aura donc un faible niveau de granularité.

Cet exercice de collecte, de formalisation et d'évaluation des risques par les principaux responsables d'un organisme d'assurance se fait généralement par entretien et/ou questionnaire ouverts. L'idée étant que ces dirigeants s'expriment sur leur vision des risques pesant sur l'organisation et leur domaine de responsabilité. Ce type d'analyse peut-être réalisée à travers la formalisation de scénarios.

L'exercice de normalisation (rattachement au référentiel des risques, et des processus de l'organisation) et de hiérarchisation pourra se faire dans un second temps.

#### *3.3.2.2 Rapprochement avec la nomenclature des risques de l'organisation*

Généralement, l'identification des risques se fait avec le top management par entretien, avec des questions ouvertes (ex. : citer les 3 principaux risques pouvant affecter l'entreprise, citer les 3 principaux risques pouvant affecter votre domaine de responsabilité). Aussi, pour permettre de consolider les résultats et proposer une vision exhaustive des risques, le rattachement à la nomenclature des risques de l'organisation est à prévoir.

#### *3.3.2.3 Lien avec les processus de l'organisation*

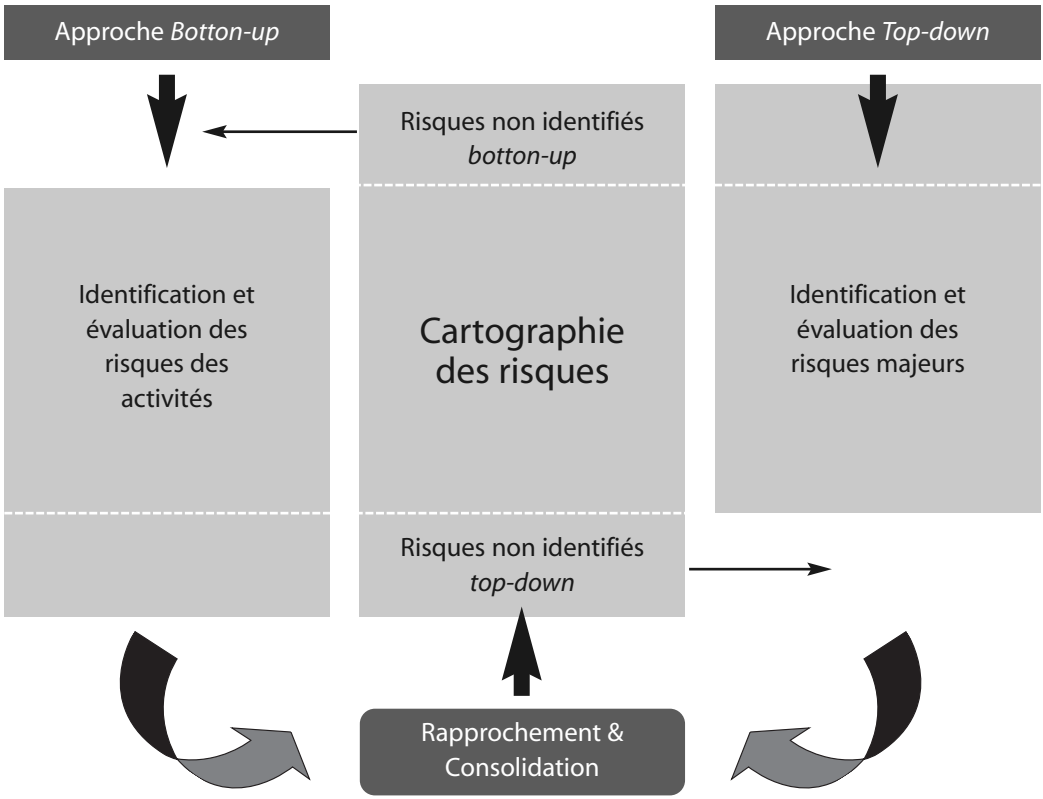
Le rattachement des risques au processus est une étape nécessaire pour permettre les regroupements et les consolidations.

Au cours de cette phase, il s'agit de remplir le double objectif de mise en cohérence des risques identifiés avec les activités de l'entité et d'exhaustivité de l'analyse.

### 3.3.3 Intégration des deux démarches

Les démarches *top-down* et *bottom-up* sont des démarches complémentaires qui doivent être combinées et développées dans les organisations afin de couvrir au mieux l'ensemble des risques. Ces deux méthodes ont vocation à alimenter et faire vivre la cartographie des risques de l'organisation.

© IFACI




En effet, ces deux approches, non seulement ne s'opposent pas, mais sont complémentaires. Elles peuvent être conduites soit de façon successive, soit de façon simultanée, la question du choix pouvant se poser lors du démarrage d'un projet de cartographie, les avantages et les inconvénients de ces démarches sont résumées ci-après.

La **méthode** ***bottom-up*** présente au moins les trois avantages suivants :

- L'approche par les processus permet d'obtenir une bonne connaissance des activités de l'entreprise et les résultats peuvent ensuite être utilisés à d'autres fins, dans le cadre d'une réorganisation ou à l'occasion d'une démarche qualité.
- L'analyse dans le détail des activités permet d'améliorer l'exhaustivité du recensement des risques.
- La consultation des opérationnels pour la réalisation de la cartographie permet d'obtenir une implication satisfaisante de leur part.



© IFACI

En revanche, c'est une démarche consommatrice de temps dans la mesure où elle requiert la tenue de nombreux entretiens et la collecte d'informations en masse. Par ailleurs, elle peut s'avérer coûteuse en termes de compétences et de systèmes car la collecte de ces données nécessite souvent le recours à des outils informatiques.

Quant à l'**approche** ***top-down***, elle permet une mise en œuvre plus légère puisque les entretiens nécessaires sont moins nombreux. L'examen des risques stratégiques permet également de s'assurer de la prise en compte plus immédiate des processus transversaux ou managériaux, ce qui peut être plus en adéquation avec les attentes de la direction générale.

Cependant, elle présente l'inconvénient d'être moins précise, tant dans l'identification des risques que dans leur quantification. Par ailleurs, les opérationnels n'étant pas associés, ils peuvent avoir du mal à s'approprier la démarche.

Enfin, il convient de préciser que, quelles que soient la ou les méthodes utilisées, nous ne pouvons jamais être certains de couvrir l'exhaustivité des risques.

#### *3.3.3.1 Consolider et hiérarchiser les principaux risques*

Ces deux démarches complémentaires doivent alimenter et faire vivre la cartographie des risques de l'organisation. Le rapprochement et la consolidation des éléments issus de ces deux méthodes seront facilités par l'utilisation d'un corpus commun et cohérent en termes de nomenclature des risques, de référentiel des processus de l'organisation et de règles de quantification.

Cette consolidation permettra de hiérarchiser les risques, d'identifier les principaux risques (significatifs et/ou élevés) et de fournir les éléments nécessaires à la prise de décision.

#### *3.3.3.2 Décider des mesures de traitements*

Face à un risque, quatre types de décision peuvent être prises :

1. **Acceptation :** le risque est accepté soit lorsque celui-ci entre dans la politique de gestion des risques de l'organisation (par exemple, acquisition d'un nouveau portefeuille de contrats, sachant que celui-ci présente un risque de dérive de la sinistralité connue) ; soit lorsque les coûts de mises en œuvre des éléments de maîtrise deviennent trop excessif au regard du risque encouru.

© IFACI

2. **Réduction :** cette mesure vise à réduire le risque sans nécessairement le faire totalement disparaitre. En effet, des actions correctives ou préventives peuvent être mises en place pour réduire ou maitriser le risque.

3. **Evitement :** cette action consiste à éliminer le risque, c'est-à-dire sa probabilité de survenance. Par exemple, la décision de ne pas acquérir un portefeuille de contrats déficitaire apportant des pertes financières supérieures aux gains escomptés.

4. **Partage :** certains risques peuvent être partagés, par exemple par la souscription d'une couverture d'assurance (ex. : garantie perte d'exploitation en cas de sinistre dans un bâtiment de l'entreprise), la mise en place d'un traité de réassurance (ex. : pour céder un risque de souscription) ou encore la sous-traitance de certaines activités (ex. : externalisation de la gestion d'une tâche afin de garantir les délais).

Le traitement d'un risque peut générer d'autres risques, il est donc important de prendre en considération les effets en cascade.

### *3.3.3.3 Concevoir, mettre en place et suivre les plans d'actions*

Les décisions prises font l'objet de la définition et de la mise en place de plans d'actions. Ces derniers devront être formalisés et rattachés aux risques identifiés. Un dispositif de suivi de ces plans d'actions devra être mis en place, et constituera ainsi un des éléments de suivi permanent des risques.

| BOITE À OUTILS | |
|---|---|
| **Pour la mise en place d'une démarche de cartographie des risques : une structure projet indispensable** | • Un « Sponsor» au niveau de la direction générale assure l'interface et la promotion du projet.<br>• Un « Comité de Pilotage » peut intégrer des représentants de fonctions impliquées dans la démarche de cartographie. Son rôle sera de suivre le déploiement et de valider les orientations, décisions et livrables qui lui seront proposés.<br>• Une « équipe projet » prend en charge la réalisation de la démarche et aura pour tâche essentielle de coordonner l'ensemble des moyens matériels et humains nécessaires à la réussite du projet.<br>• Une liste d'« interlocuteurs clés », à identifier pour participer aux entretiens et ateliers. |



© IFACI

| BOITE À OUTILS | |
|---|---|
| **Pour pérenniser la démarche : définir une organisation** | Passé le premier exercice de cartographie, la question de son utilisation effective et de sa pérennisation se pose. L'organisation suivante contribue à cette pérennisation :<br>• Un point central, le « risk manager », qui anime le dispositif dans le temps et assure la cohérence des démarches et les *reporting*.<br>• Un réseau de « propriétaire de risques » peut compléter le dispositif.<br>• Un comité de suivi des principaux risques et des plans d'actions associés doit être défini et mis en œuvre. |
| **Pour une approbation de la cartographie des risques et de la démarche** | La cartographie des risques doit faire l'objet d'une approbation formelle au niveau des différents responsables concernés, puis au niveau de la direction générale. Cette validation peut intervenir sur présentation d'un dossier de synthèse pouvant contenir des éléments tels que :<br>• La synthèse des travaux.<br>• Une présentation détaillée des travaux. |

Exemples d'éléments à présenter pour la validation de la cartographie des risques pour :

| | |
|---|---|
| **La synthèse des travaux** | • l'objectif de la démarche,<br>• le périmètre analysé,<br>• une présentation synthétique du résultat des travaux (nombre de risques, leur nature, leur évaluation, etc.). |
| **Une présentation détaillée des travaux** | • une description des processus,<br>• un focus sur les risques critiques,<br>• une présentation des éléments de maîtrise,<br>• une présentation des plans d'actions. |

© IFACI

© IFACI

# Partie 4

# Suivi permanent des risques

Dans le cadre du suivi permanent des risques, il est nécessaire de mettre en œuvre et de s'appuyer sur un certain nombre d'outils :

- le suivi de la mise en œuvre des plans d'actions ;
- la réalisation de « plan de contrôles ou de tests », afin de vérifier que les éléments de maîtrise ont effectivement été conformément mis en œuvre ;
- la mise en place d'une base d'incidents afin de recenser les événements susceptibles d'avoir un impact négatif pour l'organisation ;
- la définition et la mise en place de ratios économiques ou d'indicateurs de suivi de l'évolution des risques.

Ces éléments sont nécessaires d'une part à l'actualisation de la cartographie des risques et d'autre part à alimenter des ***reporting*** internes ou externes.

Avoir finalisé la cartographie des risques représente une étape essentielle dans la mise en œuvre du dispositif de contrôle interne. Encore faut-il, ensuite, faire vivre cette cartographie des risques, en l'actualisant régulièrement. A défaut, et compte tenu de la rapidité de l'évolution de la vie de l'entreprise, cette cartographie deviendrait rapidement inopérante et l'organisme d'assurance perdrait le bénéfice de l'investissement réalisé au départ. Mais, là aussi, cela nécessite d'allouer un minimum de ressources à la maintenance de cet outil.
Enfin, des facteurs tels que les évolutions réglementaires, les nouveaux risques, les incertitudes croissantes liées à l'environnement, rendent indispensables cette actualisation.

© IFACI

## 4.1 Une modalité particulière de suivi à partir de la base d'incidents

Un incident est un événement d'origine interne ou externe ayant un impact négatif pour l'organisation. L'absence ou le dysfonctionnement des procédures peut se traduire par :

- des pertes financières ;
- une atteinte à l'image ou la réputation ;
- des incidences juridiques ou de conformité (une mise en cause judiciaire ou une sanction pour non-respect des réglementations applicables).

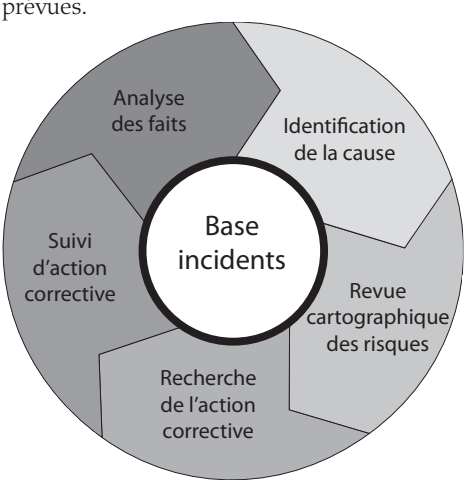
L'objectif d'une base d'incidents n'est pas d'identifier les responsables « personnes physiques » d'un incident dans le but de les sanctionner. De ce fait, à ce titre, elle doit être dépourvue de toute donnée nominative.

La base d'incidents permet :

- de recenser et centraliser l'ensemble des incidents survenus ;
- de détecter des éléments de maîtrise inefficaces ou des risques non identifiés dans la cartographie des risques ;
- d'enregistrer et suivre les mesures correctives prises en conséquence ;
- de contribuer à la connaissance des principaux risques de l'organisme d'assurance ;
- d'identifier les zones de vulnérabilité et de permettre la mise en place de dispositifs de contrôles adéquats ;
- d'alimenter les modèles statistiques qui permettent de dimensionner plus précisément les montants de fonds propres à mobiliser pour couvrir le risque opérationnel dans le cadre de *Solvabilité II* ;
- de mettre ainsi à jour également la cartographie des risques.

Les données collectées sont classées de façon structurée : cause, événement, impact, et les actions et/ou solutions mises en œuvre à effet immédiat ou prévues.

L'exploitation de la base d'incidents s'inscrit dans une logique de cercle vertueux en s'appuyant notamment sur la cartographie des risques en vérifiant que le risque survenu a été identifié, et en appréciant la performance des éléments de maîtrise réputés en place, et sur les actions correctives relatives à l'incident.






© IFACI

Une fiche de restitution peut être établie afin d'informer de manière transverse les différents acteurs concernés directement ou indirectement par la problématique résultant d'un incident traité. Ce principe de « fiche de restitution » s'inscrit dans un objectif de non-reproduction de l'incident, empruntant ainsi une démarche d'amélioration continue.

L'alimentation de la base repose sur l'organisation d'un maillage adéquat des entités qui permettra l'identification, l'analyse, la remontée et la validation des événements. Dès lors, il convient de définir avec précision :

- les typologies nécessaires à la description de l'incident (origine, détection, conséquences, impact) ;
- le dispositif, les rôles et responsabilités de chacun ainsi que les modalités de remontée des incidents :
- une attention particulière doit être accordée au rôle des activités « connexes » au contrôle interne (contrôle qualité, par exemple) en matière de remontée d'incident,
  - les incidents transverses (incidents détectés par une entité mais relevant d'une autre) doivent faire l'objet d'une procédure spécifique ;
  - les modalités d'enregistrement ;
- les modalités de chiffrage de l'impact financier ;
- les règles de rapprochement avec la cartographie des risques (imputer l'incident au risque selon le référentiel en place et le lier au processus concerné).

A propos de la gestion des incidents informatiques, se reporter au GTAG 6 : Gérer et auditer les vulnérabilités des technologies de l'information et à l'annexe 6.

## 4.2 Une communication appropriée

Une cartographie des risques n'aurait aucune raison d'être si son contenu ne servait à fournir des informations appropriées à un certain nombre de destinataires. Le *reporting* permet donc de rendre compte des travaux et de faire vivre la démarche.

Illustrations des modes de *reporting* en annexe 10.

Ces remontées d'informations matérialisent l'insertion de la cartographie des risques dans le dispositif de gestion des risques. Elles sont intégrées aux informations nécessaires à un pilotage adapté et réactif des activités. Elles participent également à la production de *reporting* de plus en plus détaillés et denses requis par la réglementation, et plus particulièrement par l'ACP.

Ces *reporting* interne et externe doivent être **adaptés** aux destinataires.

© IFACI

## 4.2.1 *Reporting* interne

Pour un déploiement des cartographies des risques dans la durée et pour accroître leur fiabilité, il est indispensable qu'elles trouvent des clients.

### *4.2.1.1 Répondre aux attentes des managers*

Acteur clé des dispositifs de gestion des risques et de contrôle interne, le management s'appuie sur différents éléments et indicateurs clés pour diffuser la sensibilité aux risques **dans son périmètre de responsabilité,** et ainsi faire connaître les objectifs de gestion des risques.

Les managers ont généralement besoin d'avoir accès à des synthèses concernant :

- les travaux de cartographies relatifs à leur domaine de responsabilité avec un zoom sur :
  - les risques majeurs identifiés et/ou faisant l'objet d'une maîtrise insuffisante,
  - les mêmes risques classés par nature en lien avec le référentiel de risque (technique, opérationnels, externes, etc.),
  - les plans d'optimisation de la maîtrise par ordre de priorité et le suivi du respect des échéances associées.
- les contrôles clés leur permettant notamment de suivre :
  - les taux de réalisation,
  - les taux d'anomalie (notamment par rapport au seuil de tolérance),
  - les corrections apportées.
- les incidents :
  - le nombre et la récurrence des incidents,
  - le délai de traitement,
  - les pertes financières directes ou indirectes générées.
- les plans d'actions :
  - les actions échues,
  - les actions réalisées,
  - le respect des échéances,
  - le taux d'avancement global des actions en-cours, etc.

En complément, le management organise le suivi d'indicateurs sur les risques clés (KRI – *Key Risk Indicators*), et sur des points sensibles des activités dont il porte la responsabilité.

### *4.2.1.2 Reporting à l'usage des acteurs de la seconde ligne*

L'action des managers opérationnels est renforcée par celles des acteurs de la deuxième ligne de défense. Certains de ces acteurs sont amenés à communiquer le niveau de maîtrise des risques aux instances dirigeantes de l'organisme via notamment :



© IFACI

- une vision consolidée des cartographies des risques (nombre de risques, leur nature, leur évaluation, etc.) ;
- un focus sur les risques critiques insuffisamment maîtrisés ;
- une présentation des plans d'actions et un suivi du respect des échéances.

La fonction « gestion des risques » joue un rôle clé en élaborant des *reporting* sur le respect des métriques définit par l'organisme d'assurance :

- Indicateurs par famille de risques sur la base des limites fixées (appétence et seuils de tolérance aux risques).
- Alerte déployée en cas de dépassement de l'allocation de capital définie dans l'appétence aux risques.

Au titre de l'animation permanente du contrôle interne, il s'agit de recueillir des informations sur les incidents, les contrôles-clés et les plans d'actions associés. C'est la consolidation de ces informations qui permettra d'alimenter le *reporting* aux managers.

En fonction des besoins, l'organisme d'assurance pourra élaborer des *reporting* par grand domaine tel que :

- la fraude ;
- la protection de la clientèle dont le suivi des réclamations ;
- la protection des données confidentielles ;
- la sécurité des biens et des personnes ;
- la lutte contre le blanchiment et le financement du terrorisme (LCB-FT),
- etc.

Autant que possible, ces *reporting* seront conçus de manière à pouvoir optimiser la production des *reporting* externes.

En outre, la fonction « actuarielle » pourra élaborer des *reporting* concernant :

- la qualité des provisions techniques ;
- le caractère approprié des méthodologies, des modèles sous-jacents et des hypothèses utilisés ;
- la qualité des données et des hypothèses retenues.

Selon les structures, la fonction « actuarielle » peut également s'assurer que les stratégies d'investissement déployées découlent d'une analyse des équilibres actifs / passifs : elle produit alors des études sur les flux de trésorerie et de rendement, sur l'adéquation des durations entre actifs et passifs, sur l'évolution d'indicateurs financiers, et des études de scénarios de risques.

© IFACI

### 4.2.1.3 Source d'information pour l'audit interne

Sur la base d'un plan d'audit fondé sur une approche par les risques, l'audit interne apporte une opinion sur l'efficacité des processus de contrôle interne, de gestion des risques et de gouvernance. En particulier, l'audit interne, peut à partir de la cartographie des risques de l'organisme d'assurance (y compris l'analyse de la base d'incidents) :

- prendre en compte les principaux risques identifiés ;
- utiliser les données concernant les risques associés aux processus qu'il évalue au cours de ses missions.

L'audit interne contribue également au *reporting* interne sur les risques en :

- s'assurant du niveau de couverture de l'identification des risques ;
- vérifiant l'existence et le bon fonctionnement des éléments de maîtrise ;
- rendant compte de ses travaux à la direction générale, au comité d'audit et au Conseil.

Ces éléments permettent d'actualiser la cartographie des risques.

### 4.2.1.4 Reporting *à destination des organes dirigeants et délibérants*

Pour mener à bien leurs missions, les organes dirigeants et délibérants s'appuient sur différents *reporting* et indicateurs. Il s'agit d'adapter la conduite de l'organisme à son environnement interne et externe, et au niveau de risque associé.

La directive oblige chaque organisme d'assurance à mettre en place un système de gestion des risques efficace[1], parfaitement intégré à la structure organisationnelle et aux procédures de prise de décision. Il doit donc être dûment pris en compte par les dirigeants. Cela nécessite donc une **intégration aux tableaux de bords des organismes d'assurance** de tous les éléments relatifs à la gestion des risques (**agrégats économiques macro, analyse des principaux risques** existants et potentiels auxquels est exposé l'organisme).

De plus, les tableaux de bords devront intégrer une dimension prospective : à l'aide de modèles de simulations, chaque organisme d'assurance devra projeter sa situation financière sur l'horizon du plan stratégique en prenant en compte plusieurs hypothèses d'évolution du contexte économique (projections des bilans, comptes de résultat, SCR – *Solvency Capital Requirement*, MCR – *Minimum Capital Requirement*, indicateurs du profil de risques, etc.).

Ces projections serviront d'outil d'aide à la décision pour l'organe dirigeant afin d'assurer sur le long terme l'adéquation entre la prise de risque et la solvabilité.

[1] *Article 44 de la directive Solvabilité II (cf. annexe 7)*



© IFACI

## 4.2.2 *Reporting* externe

Compte tenu du cadre réglementaire rappelé dans la partie 1.3, les organismes d'assurance sont soumis à des obligations de *reporting* de plus en plus précis.

### *4.2.2.1 Reporting en réponse aux exigences de l'ACP*

Actuellement, les éléments ci-après doivent être établis et communiqués à l'ACP. Ces éléments intègrent pour partie les résultats et les travaux opérés dans les démarches de cartographies des risques :

- rapports réglementaires (états financiers, rapport de gestion, rapport de solvabilité, rapport sur le contrôle interne, rapport d'intermédiation) ;
- états prudentiels.

Un point sur la directive *Solvabilité II* est proposé ci-après, afin d'identifier les principales évolutions à venir sur ce domaine.

### *4.2.2.2 Préparer Solvabilité II*

Les éléments de *reporting* externes sont définis dans le Pilier 3 de la directive et le périmètre des *reporting* concernés est celui décrit dans le document de travail du CEIOPS « CP58[1] ».

Les organismes d'assurance devront produire un ensemble de rapports annuels, qualitatifs et quantitatifs ; à destination du régulateur et du public, remplacement de certains états de *reporting* prudentiel et les rapports narratifs de solvabilité et de contrôle interne :

1- **RSR** *(Regular supervisory report)* : Rapport destiné à l'ACP comprenant un rapport narratif et les états quantitatifs (annuels et trimestriels, notamment les QRT - *Quantitative Reporting Template*). L'objectif du RSR est double : servir de base aux éventuels contrôles et mesurer les risques systémiques.

2- **SFCR** *(Solvency and financial condition report)* : Rapport diffusé au public comportant la structure du RSR sans les informations à destination des régulateurs. L'objectif est d'accroître également la transparence des informations, et de renforcer la discipline de marché.

3- **Rapport ORSA** *(Own Risk and Solvency Assesment)* : Rapport présentant :
   - les résultats qualitatifs et quantitatifs du dispositif ORSA,
   - les méthodes et principales hypothèses utilisées,

[1] *CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Supervisory Reporting and Public Disclosure Requirements – (former Consultation Paper 58)*

© IFACI

- des informations sur le besoin global de solvabilité évalué par l'ORSA,
- une comparaison entre le besoin global en solvabilité, les exigences règlementaires de capital (SCR et MCR) et les fonds propres,
- une information si besoin sur les risques non compris dans la formule standard comme les risques stratégiques, de réputation ou encore extrêmes.



© IFACI

# CONCLUSION

© IFACI

La cartographie n'est pas une fin en soi. Elle doit s'inscrire dans le cadre du pilotage global de l'organisation tout en contribuant à la conformité réglementaire.

Même si les dirigeants et les managers ont une vision globale des risques inhérents à leurs activités, construire une cartographie des risques leur apportera de nouveaux éléments d'observation destinés à mieux maîtriser et orienter leurs objectifs.

Ainsi, la dimension « risques » vient enrichir la vision des dirigeants en complément des axes stratégiques et opérationnels et devient un élément de management à part entière.

Les applications d'une cartographie des risques sont nombreuses et conduisent les utilisateurs à privilégier tel ou tel aspect des résultats obtenus afin de redéfinir leurs priorités.

Du conseil d'administration à la direction générale, en passant par les responsables opérationnels, les risk managers, les contrôleurs internes et les auditeurs internes, chacun pourra utiliser la cartographie comme support à des actions propres à leur organisation.

Pour ce faire, les organismes d'assurance doivent instaurer un environnement permettant d'aboutir à des cartographies des risques fidèles et dynamiques.

Les facteurs clés de succès pour faire de la cartographie des risques un outil au service du pilotage du dispositif de gestion des risques et un élément d'aide à la décision sont :

- une clarification des acteurs et de la gouvernance ;
- un *sponsoring* par la direction générale et le comité de direction ;
- une sensibilisation et la diffusion de la culture des risques à tout niveau ;
- une documentation du fonctionnement de l'entreprise (« qui fait quoi ? », procédures, fiches de fonction, etc.) ;
- la formalisation de la stratégie de l'organisme d'assurance et d'un plan d'affaires à moyen terme ;
- une responsabilisation des managers sur ces questions ;
- une organisation en mode projet lors du lancement de toute démarche.

Conscient de l'apport potentiel des outils informatiques dans ce type de démarche, le groupe de travail attire néanmoins l'attention sur l'importance d'une identification préalable des besoins spécifiques à chaque organisme. Lorsque l'option retenue est d'acquérir un progiciel plutôt que de développer en interne une solution informatique, le dialogue avec les éditeurs et la gestion de l'outil devront s'appuyer sur les fondamentaux de la gestion de projets et les échanges de bonnes pratiques avec des pairs[1].

Le succès d'une cartographie des risques réside dans son utilisation effective, dans la capacité des utilisateurs à la faire vivre dans le temps. C'est dans ce sens que le référentiel commun qui vous a été présenté a été construit.

[1] *Cf. les bonnes pratiques proposées dans le cahier Sélectionner un outil informatique pour les services d'audit et de contrôle internes de l'unité de recherche « Informatique » de l'IFACI (2013), les clubs d'utilisateurs ou les articles dans la revue de l'IFACI.*



© IFACI

# ANNEXES



© IFACI

# ANNEXE 1

## Exemples de processus - Secteur assurances

**Développer l'offre**

- Analyse du marché : concurrence, besoins des clients, tendance, nouveaux marchés
- Définition du produit : quel type de produit, à destination de qui, pour quel vecteur de distribution
- Elaboration du produit : conditions générales ; tarifaires
- Lancement de l'offre : communication externe, publicité, événementiel, formation des forces de ventes)

→ **Nouvelle offre**

**Vendre**

- Déclinaison de la politique commerciale et pilotage
- Animation des réseaux de distribution
- Etablissement des propositions tarifaires
- Négociation
- Enregistrement et émission des pièces contractuelles
- Envoi et archivage

→ **Pièces contractuelles**

**Gérer le contrat**

- Enregistement du contrat dans l'outil de gestion
- Appel de cotisations
- Encaissement des cotisations
- Gestion de la trésorerie
- Mise à jour des données contrat
- Gestion des avenants (analyse du dossier, avis médical, enregistrement et émission, envoi et archivage)
- Gestion des bénéficiaires
- Suivi des impayés (relance, contentieux)
- Rémunération des tiers (intermédiaires, gestionnaires)

→ **Chiffre d'affaires**

**Traitement de fin d'année**

- Etablissement des attestations fiscales (Madelin, rentiers, apporteurs)
- Revalorisation annuelle (dont hausse tarifaire)
- Inventaire

→ **Etats**

**Gérer les prestations**

- Paramétrage des garanties
- Instruction et contrôle
- Constitution du dossier
- Contrôles médicaux
- Calcul du montant
- Règlement
- Réassureur
- Recours contre tiers
- Actualisation des dossiers (maintien, clôture, demande de justificatif )
- Provisionnement

→ **Paiement sinistres**

**Maîtriser les résultats des contrats**

- Inventaire
- Statisitques
- Révisions tarifaires
- Redressement

→ **Contrats renégociés**





© IFACI

# ANNEXE 2

## Nomenclature des risques



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R101 | Risques de solvabilité | Risques résultant d'un niveau des fonds propres et quasi-fonds propres inférieur au minimum réglementaire |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R101 | Risques de solvabilité | Risques résultant d'un niveau des fonds propres et quasi-fonds propres inférieur au minimum réglementaire |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R101 | Risques de solvabilité | Risques résultant d'un niveau des fonds propres et quasi-fonds propres inférieur au minimum réglementaire |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R102 | Adéquation Actif / Passif | Risques résultant d'une inadéquation, en montant ou en structure, entre le passif correspondant aux engagements pris envers les clients et l'actif mis en représentation |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R10101 | Risques de solvabilité réglementaire en social | Risques résultant d'un niveau des fonds propres et quasi-fonds propres inférieur au minimum réglementaire en social pour chaque entité | | | Solvabilité globale |
| R10102 | Risques de solvabilité réglementaire en consolidé | Risques résultant d'un niveau des fonds propres et quasi-fonds propres inférieur au minimum réglementaire dans les comptes consolidés (solvabilité ajustée) | | | Solvabilité globale |
| R10103 | Risques de solvabilité de marché | Risques résultant d'un niveau des fonds propres et quasi-fonds propres inférieur au montant estimé par les analystes ou les marchés financiers entraînant un seuil de déclenchement de "triggers" | | | Solvabilité globale |
| R10201 | Risques de liquidité | Correspond à une évolution du passif à court terme engendrant des insuffisances d'actifs réalisables | Marché | | ALM |
| R10202 | Risques de limitation par catégorie d'actif ou de passif | Correspond à un manque de diversification, tant à l'actif qu'au passif, qui conduit à une exposition trop forte sur un risque particulier (type de risque assuré, risque de taux, risque actions, etc.) | Marché | | ALM |
| R10203 | Risques de disparités de lignes de passifs | Correspond à une structure de passif éclatée et difficile à mettre en adéquation avec des actifs | Marché | | ALM |
| R10204 | Risques de couverture imparfaite | Se matérialise par une inadaptation ou une insuffisance de la structure des actifs au regard de celle des passifs | Marché | | ALM |
| R10205 | Risques de taux | Risques d'inadéquation actif / passif provenant du comportement des marchés de taux | Marché | | ALM |
| R10206 | Risques actions | Risques d'inadéquation actif / passif provenant du comportement des marchés d'actions | Marché | | ALM |
| R10207 | Risques de change | Risques d'inadéquation actif / passif provenant du comportement des marchés de devises | Marché | | ALM |
| R10208 | Risques immobiliers | Risques d'inadéquation actif / passif provenant du comportement des marchés immobiliers | Marché | | ALM |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R10301 | Risques de trésorerie | Résulte d'un manque de liquidités disponibles à court terme pour faire face aux obligations de règlement | Marché | | Liquidité |
| R10302 | Risques de refinancement | Est la conséquence d'une inadéquation ou d'un défaut de financement permettant d'obtenir les liquidités suffisantes pour faire face aux obligations de règlement | Marché | | Liquidité |
| R10303 | Risques de concentration | Correspond à un manque de diversification dans le placement des actifs qui conduit à une exposition trop forte sur un risque particulier (actions, taux, crédit) | Marché | Concentration | |
| R10304 | Risques de taux | Conséquence d'une évolution des taux d'intérêt sur la valeur des actifs obligataires | Marché | Taux | |
| R10305 | Risques de change | Est lié à la variation de valeur d'une devise par rapport à l'euro, et à l'impact de cette variation sur la valeur des actifs en devises | Marché | Change | |
| R10306 | Risques actions | Conséquence d'une évolution des marchés actions, ou d'une trop forte dépendance vis-à-vis de ce type d'actif | Marché | Action | |
| R10307 | Risques immobiliers et fonciers | Conséquence d'une évolution des marchés immobiliers et fonciers, ou d'une trop forte dépendance vis-à-vis de ce type d'actif | Marché | Immobilier | |
| R10308 | Risques de contrepartie | Découle du défaut de la contrepartie à une opération, au moment où elle doit remplir ses obligations (absence de paiement à l'échéance, etc.) | Contrepartie | | |
| R10309 | Risques émetteur | Lié au défaut de l'émetteur préalablement à la réalisation de ses obligations (remboursement d'un emprunt à l'échéance, etc.) | Contrepartie | | |
| R10310 | Risques crédit | Correspond à la variation de la qualité de crédit d'un émetteur conduisant à l'augmentation de la prime de risque attendue par ses créanciers | Contrepartie | | |
| R10311 | Risques d'évaluation d'actifs | Risques résultant de la surestimation d'un élément d'actif, pouvant entraîner notamment une constatation de moins-value en cas de cession ou d'ouverture de capital, ou un provisionnement suite à révision | Marché | | Allocation d'actif (concerne le non coté) |
| R10312 | Risques de rentabilité insuffisante des participations et filiales | Risques résultant d'un niveau de rentabilité annuelle insuffisant pour amortir les coûts d'acquisition | | | Stratégique |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R103 | Gestion d'actifs | Risques relatifs à la gestion des actifs |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R104 | Endettement | Risques résultant d'un endettement trop important eu égard aux charges de remboursement ou aux taux des emprunts en cours |
| R1 | Financiers | Risques liés à l'évolution des marchés financiers, de gestion de bilan ou financière | R104 | Endettement | Risques résultant d'un endettement trop important eu égard aux charges de remboursement ou aux taux des emprunts en cours |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R201 | Technique | Risques résultant de caractéristiques des produits nuisant à leur rentabilité (provenant ou non de la réalisation de risques production ou marketing) |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R201 | Technique | Risques résultant de caractéristiques des produits nuisant à leur rentabilité (provenant ou non de la réalisation de risques production ou marketing) |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R201 | Technique | Risques résultant de caractéristiques des produits nuisant à leur rentabilité (provenant ou non de la réalisation de risques production ou marketing) |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R202 | Souscription | Risques relatifs à la souscription de contrats d'assurance, ou à l'acceptation de traités ou facultatives de réassurance, hors sinistralité et prestations |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R202 | Souscription | Risques relatifs à la souscription de contrats d'assurance, ou à l'acceptation de traités ou facultatives de réassurance, hors sinistralité et prestations |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R202 | Souscription | Risques relatifs à la souscription de contrats d'assurance, ou à l'acceptation de traités ou facultatives de réassurance, hors sinistralité et prestations |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R202 | Souscription | Risques relatifs à la souscription de contrats d'assurance, ou à l'acceptation de traités ou facultatives de réassurance, hors sinistralité et prestations |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R202 | Souscription | Risques relatifs à la souscription de contrats d'assurance, ou à l'acceptation de traités ou facultatives de réassurance, hors sinistralité et prestations |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R10313 | Risques crédit réassureurs | Risque de défaillance d'un réassureur réduisant ses capacités à remplir ses engagements | Contrepartie | | |
| R10401 | Risques d'endettement inadéquat | Niveau d'endettement du Groupe inexistant, l'empêchant d'optimiser ses ressources ou sa rentabilité | | | Stratégique |
| R10402 | Risques de surendettement | Niveau d'endettement du Groupe trop élevé, pouvant entraîner une crise de liquidité ou rendre impossible le financement de la croissance du Groupe | | | Stratégique |
| R20101 | Risques de définition produit (contrat d'assurance ou traité de réassurance en acceptation) | Risques provenant d'une définition des conditions d'assurance ou de réassurance impropres à une viabilité économique (quelle que soit la tarification) | Souscription | | |
| R20102 | Risques de tarification (assurance ou réassurance acceptée) | Risques issus de tarifs soit insuffisants par rapport au coût réel des garanties et frais de gestion, soit trop élevés et générateurs d'anti-sélection | Souscription | Primes et réserves | |
| R20103 | Risques de non-rentabilité des produits d'assurance ou des traités de réassurance acceptés | Risques de non-rentabilité à moyen ou long terme | Souscription | Primes et réserves | |
| R20201 | Risques de qualité insuffisante de l'objet risque | Souscriptions de mauvaise qualité, quant aux risques soucrits, malgré leur conformité aux règles | Souscription | | |
| R20202 | Risques de cumul de souscription | Dépassement des engagements acceptables sur un même site, un même client, ou un même risque d'assurance | Souscription | | |
| R20203 | Risques de cumul souscription / actif | Effets cumulatifs dus à la dépendance ou la corrélation entre des risques de souscription et des risques sur les actifs | Souscription | Primes et réserves | |
| R20204 | Risques d'apérition | Risques relatifs à la gestion des coassurances ou des coréassurances | Souscription | | |
| R20205 | Risques de coassurance non apéritrice ou coréassurance suiveuse | Risques de mauvaise gestion ou d'informations insuffisantes émanant de l'apériteur ou du coréassureur leader | Souscription | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R202 | Souscription | Risques relatifs à la souscription de contrats d'assurance, ou à l'acceptation de traités ou facultatives de réassurance, hors sinistralité et prestations |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R203 | Sinistralité non vie / Prestations vie | Risques résultant d'une déviation de la charge sinistres ou prestations compromettant l'équilibre attendu entre primes et charges techniques des portefeuilles |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R203 | Sinistralité non vie / Prestations vie | Risques résultant d'une déviation de la charge sinistres ou prestations compromettant l'équilibre attendu entre primes et charges techniques des portefeuilles |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R203 | Sinistralité non vie / Prestations vie | Risques résultant d'une déviation de la charge sinistres ou prestations compromettant l'équilibre attendu entre primes et charges techniques des portefeuilles |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R203 | Sinistralité non vie / Prestations vie | Risques résultant d'une déviation de la charge sinistres ou prestations compromettant l'équilibre attendu entre primes et charges techniques des portefeuilles |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R203 | Sinistralité non vie / Prestations vie | Risques résultant d'une déviation de la charge sinistres ou prestations compromettant l'équilibre attendu entre primes et charges techniques des portefeuilles |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R204 | Provisionnement | Risques résultant d'un provisionnement inadapté à l'évolution de la charge sinistres et prestations en cours ou à venir |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R204 | Provisionnement | Risques résultant d'un provisionnement inadapté à l'évolution de la charge sinistres et prestations en cours ou à venir |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R204 | Provisionnement | Risques résultant d'un provisionnement inadapté à l'évolution de la charge sinistres et prestations en cours ou à venir |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R205 | Participations aux bénéfices | Risques relatifs aux participations aux bénéfices attribuées aux assurés vie |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R206 | Réassurance de protection | Risques résultant des conditions négociées avec les réassureurs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R20206 | Risques d'annulation, de résiliation, de réduction | Fréquence élevée de chute ou de réductions de contrats (arrêt du paiement des primes) | Souscription | Rachat | |
| R20301 | Risques de déviation de la sinistralité | Evolution défavorable de la charge sinistre dans une ou plusieurs catégories d'assurance, d'une façon plus ou moins rapide (augmentation de fréquence ou d'intensité) | Souscription | Primes et réserves | |
| R20302 | Risques de fréquence des sinistres de pointe | Survenance plus fréquente qu'attendue, de sinistres de montant élevé | Souscription | Primes et réserves | |
| R20303 | Risques de cumul de sinistres | Survenance d'un sinistre catastrophique, d'un cumul RC ou sériel, ou d'un cumul de sinistres entre plusieurs branches | Souscription | Catastrophe | |
| R20304 | Risques de rachat (vie) | Fréquence élevée de rachats de contrats "épargne" | Souscription | Rachat | |
| R20305 | Risques de longévité (rentes viagères) | Durée de survie des rentiers supérieure à ce qui avait été pris en compte dans les tarifs de rentes | Souscription | Longévité | |
| R20401 | Risques relatifs aux montants de provisions de primes (hors PM) | Risques résultant de provisions insuffisantes devant la charge sinistres à venir | Souscription | Primes et réserves | |
| R20402 | Risques relatifs aux montants de provisions mathématiques (PM) | Risques résultant de provisions mathématiques (PM) (vie et rente auto) insuffisantes face aux prestations à régler | Souscription | Mortalité/ Rachat/ Révision/ Longévité | |
| R20403 | Risques relatifs aux montants de provisions pour sinistres | Risques résultant de provisions pour sinistres insuffisantes devant la charge en sinistres survenus | Souscription | Primes et réserves | |
| R20501 | Risques relatifs au niveau de PB | Risques résultant d'un niveau insuffisant des attributions de PB aux assurés (au vu de la conccurence, des caractéristisques du produit, des attentes des assurés) | Souscription | | |
| R20601 | Risques d'inadéquation des couvertures de réassurance | Programme de réassurance insuffisant pour protéger correctement un portefeuille, compte tenu de la rétention supportable par l'entreprise | Souscription | Primes et réserves | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R206 | Réassurance de protection | Risques résultant des conditions négociées avec les réassureurs |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R206 | Réassurance de protection | Risques résultant des conditions négociées avec les réassureurs |
| R2 | Assurances | Risques spécifiques aux activités techniques d'assurance | R207 | Maîtrise des Résultats | Risques liés à la maîtrise des résultats |
| R3 | Opérationnels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opérationnels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opérationnels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opérationnels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opérationnels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opérationnels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R20602 | Risques de surcoût de la réassurance | Traités de réassurance tarifés trop cher | Souscription | Primes et réserves | |
| R20603 | Risques de litige avec les réassureurs | Risques de contestation de garantie par un réassureur | Souscription | Primes et réserves | |
| R20701 | Risque de dérive du ratio S/C et/ou diminution du CA | | Souscription | Primes et réserves | |
| R30101 | Conformité, diffusion d'informations et devoir fiduciaire - Acte commercial | Non-respect de la réglementation applicable à l'acte commercial | Opérationnel | | |
| R30102 | Conformité, diffusion d'informations et devoir fiduciaire - Secret professionnel | Non-respect des règles relatives aux informations privilégiées et au secret professionnel | Opérationnel | | |
| R30103 | Conformité, diffusion d'informations et devoir fiduciaire - Protection des données personnelles | Non-respect des dispositions relatives à la protection des données personnelles des personnes physiques (CNIL) | Opérationnel | | |
| R30104 | Conformité, diffusion d'informations et devoir fiduciaire - Informations confidentielles | Utilisation abusive d'informations confidentielles | Opérationnel | | |
| R30105 | Conformité, diffusion d'informations et devoir fiduciaire -Vente agressive | Pratiques de ventes agressives | Opérationnel | | |
| R30106 | Pratiques commerciales / de place incorrectes - Concurrence | Infraction à la législation sur la concurrence | Opérationnel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30107 | Pratiques commerciales / de place incorrectes - Agrément réglementaire | Défaut d'agrément réglementaire | Opération-nel | | |
| R30108 | Pratiques commerciales / de place incorrectes - LCB-FT | Non-respect des réglementations relatives au blanchiment de capitaux et au financement du terrorisme et aux obligations s'y rapportant (TRACFIN) | Opération-nel | | |
| R30109 | Pratiques commerciales / de place incorrectes - Marchés financiers | Non-respect des règles de fonctionnement des marchés financiers (déclaration en matière d'opérations suspectes, principe de l'intégrité du marché) | Opération-nel | | |
| R30110 | Pratiques commerciales / de place incorrectes - Meilleure exécution | Non-respect des règles de « meilleure exécution » des ordres | Opération-nel | | |
| R30111 | Pratiques commerciales / de place incorrectes | Non-respect des règles liées à la « ségrégation des avoirs des clients » | Opération-nel | | |
| R30112 | Pratiques commerciales / de place incorrectes - Ségrégation des avoirs des clients | Conflits d'intérêts entre deux ou plusieurs clients concernés par une même opération | Opération-nel | | |
| R30113 | Pratiques commerciales / de place incorrectes - Egalité de traitement des clients | Non-respect de l'égalité de traitement des clients | Opération-nel | | |
| R30114 | Pratiques commerciales / de place incorrectes | Non-respect du principe de primauté de l'intérêt du client | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30115 | Pratiques commerciales / de place incorrectes - Primauté de l'intérêt du client | Non-respect des dispositifs de « muraille de Chine » et non application des procédures | Opérationnel | | |
| R30116 | Pratiques commerciales / de place incorrectes - Franchissement de seuil | Franchissement de seuil et seuils de détention non déclarés | Opérationnel | | |
| R30117 | Défauts dans les produits | Mauvaise implémentation des modèles (modules de tarification, pricers, etc.) | Opérationnel | | |
| R30118 | Défauts dans les produits - Politique de tarification | Non-respect de la politique de tarification | Opérationnel | | |
| R30119 | Défauts dans les produits - Conformité des produits | Non-conformité des produits | Opérationnel | | |
| R30120 | Défauts dans les produits - Procédure de validation des nouveaux produit | Non-respect de la procédure de validation des nouveaux produits et nouvelles activités | Opérationnel | | |
| R30121 | Défauts dans les produits - Opérations complexes et sensibles | Non-respect des procédures relatives aux opérations complexes et sensibles | Opérationnel | | |
| R30122 | Contreparties commerciales | Non-respect de ses obligations par une contrepartie / un tiers (hors clientèle) | Opérationnel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Risques résultant de défaillance de qualité dans les relations avec les tiers |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R301 | Clients / tiers, produits et pratiques commerciales | Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30123 | Sponsorship exposure | Dépassement des limites d'exposition d'un client (en gestion d'actifs) | Opération-nel | | |
| R30124 | Sélection / Analyse clien-tèle | Insuffisance de l'analyse client | Opération-nel | | |
| R30125 | Risques de contractualisa-tion insuffi-sante | Risques d'absence de formalisation des rapports avec un tiers ou de contractuali-sation insuffisante | Opération-nel | | |
| R30126 | Activités de conseil | Informations inappropriées, fausses ou obsolètes délivrées aux clients | Opération-nel | | |
| R30127 | Risques de notation | Risques de mauvaise notation par une agence spécialisée | | | Réputation |
| R30128 | Risques rela-tifs aux infor-mations disponibles sur le marché | Risques de non-disponibilité des infor-mations nécessaires à la gestion des actifs | Opération-nel | | |
| R30201 | Saisie, exécu-tion et suivi des transac-tions - Erreur | Erreurs dans la saisie, le suivi ou le char-gement des données | Opération-nel | | |
| R30202 | Saisie, exécu-tion et suivi des transac-tions - Respect des procé-dures | Non-respect ou mauvaise interprétation des procédures | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30203 | Saisie, exécution et suivi des transactions - Déficiences dans l'organisation et les procédures | Déficiences dans l'organisation et les procédures internes de traitement ou de contrôle | Opération-nel | | |
| R30204 | Risques d'interface inter-services | Risques de dysfonctionnement des interfaces entre plusieurs fonctions, qu'elles s'appuient sur des moyens humains, de connectique, informatiques ou autres moyens logistiques | Opération-nel | | |
| R30205 | Saisie, exécution et suivi des transactions - Inadéquation des systèmes d'informations | Problèmes dus à l'inadéquation des systèmes d'information aux activités et produits | Opération-nel | | |
| R30206 | Saisie, exécution et suivi des transactions - Gestion des référentiels | Mauvaise gestion des référentiels | Opération-nel | | |
| R30207 | Saisie, exécution et suivi des transactions - Paramétrage | Erreur de manipulation ou de paramétrage d'un modèle / système | Opération-nel | | |
| R30208 | Saisie, exécution et suivi des transactions - Affectation comptable | Erreur d'affectation comptable (compte, entité, etc.) | Opération-nel | | |
| R30209 | Saisie, exécution et suivi des transactions - Piste d'audit | Défaut de preuve (archivage, traçabilité) / piste d'audit (SOX) | Opération-nel | | |
| R30210 | Saisie, exécution et suivi des transactions - Communication | Problèmes de communication | Opération-nel | | |
| R30211 | Saisie, exécution et suivi des transactions - Délais et obligations envers les clients | Non-respect des délais et/ou des obligations envers les clients et/ou les fournisseurs | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30212 | Saisie, exécution et suivi des transactions - Surveillance des comptes et/ou opérations | Insuffisance de surveillance des comptes et/ou des opérations | Opération-nel | | |
| R30213 | Saisie, exécu-tion et suivi des transac-tions - Traitement des réclamations | Défaillance dans le traitement des récla-mations | Opération-nel | | |
| R30214 | Saisie, exécu-tion et suivi des transac-tions - Autres | Autres causes liées aux traitements et procédures (à préciser) | Opération-nel | | |
| R30215 | Monitoring et reporting - Inexactitude d'informations communiquées à l'extérieur | Inexactitude d'informations communi-quées à l'extérieur (occasionnant des pertes) | Opération-nel | | |
| R30216 | Monitoring et reporting - Manquement à une obliga-tion déclara-tive | Manquement à une obligation déclara-tive (comptable ou réglementaire) | Opération-nel | | |
| R30217 | Monitoring et reporting - Risque de résultats erro-nés | Risque de résultat comptable et ou fiscal erroné | Opération-nel | | |
| R30218 | Documents contractuels clients - Imprécis, inadéquats ou manquants | Documents contractuels imprécis, inadé-quats ou manquants | Opération-nel | | |
| R30219 | Documents contractuels clients - Collecte et conservation | Défaillance dans la collecte et la conser-vation des dossiers et des documents relatifs aux clients | Opération-nel | | |
| R30220 | Gestion des comptes clients | Non sécurisation des accès aux comptes clients - Sécurisation | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30221 | Gestion des comptes clients - Données | Données erronées communiquées aux clients | Opération-nel | | |
| R30222 | Fournisseurs - Mauvaise exécutions des prestations | Mauvaise exécution des prestations, y compris délégataires de gestion externes | Opération-nel | | |
| R30223 | Fournisseurs - Dispositions contractuelles | Absence de dispositions contractuelles encadrant les obligations et les engage-ments pris en matière de performance par les sous-traitants | Opération-nel | | |
| R30224 | Fournisseurs - Litiges | Litiges avec les fournisseurs | Opération-nel | | |
| R30225 | Risques judi-ciaires | Risques liés à l'évolution du droit et aux décisions des tribunaux | Opération-nel | | |
| R30226 | Risques de réseau insuffi-sant | Nombre insuffisant de vendeurs pour atteindre les objectifs de vente | Opération-nel | | |
| R30227 | Risques de non-respect des limites de délégation commerciale | Abus ou non-respect de pouvoir de délé-gation de la part d'un délégataire commercial ou mandataire | Opération-nel | | |
| R30228 | Risques de commission-nement inadapté | Risques générés par un système ou une grille de commissionnement des inter-médiaires non conforme avec les objectifs de vente ou de rentabilité | Opération-nel | | |
| R30229 | Risques de défaillance d'un courtier | Risques générés par la faillite d'un cour-tier | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Risques résultant de l'intervention humaine dans les activités |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30230 | Risques de délégation de pouvoir | Mauvaise attribution de pouvoir de délégation (défaut de compétence, incohérence avec l'organisation, etc.) | Opérationnel | | |
| R30231 | Risques d'ordonnancement | Mauvaise attribution de pouvoir d'ordonnancement (défaut de compétence, incohérence avec l'organisation, etc.) | Opérationnel | | |
| R30232 | Risques relatifs à la diffusion de l'information et des données en interne | Risques de carences ou maladresses dans la diffusion des messages et des données en interne (hors logistique courrier interne) | Opérationnel | | |
| R30233 | Risques relatifs au régime de TVA et à la facturation | Risque lié à l'omission de facturation de TVA ou de déclaration | Opérationnel | | |
| R30234 | Risques relatifs à la taxation des contrats | Risques de non respect des obligations en matière de taxation des contrats d'assurance | Opérationnel | | |
| R30235 | Risques relatifs aux procédures CFCI | Risque lié à l'absence de procédure en matière de Contrôle Fiscal des Comptabilités Informatisées (CFCI) | Opérationnel | | |
| R30236 | Etats réglementaires | Risques liés à la présentation d'états réglementaires inexacts ou à la non-présentation d'états réglementaires | Opérationnel | | |
| R30237 | Risques d'engagements sur valorisation d'actifs | Risques que certains engagements reçus sur actifs soient surévalués ou ne puissent être recouvrés | Opérationnel | | |
| R30238 | Risques d'engagements sur valorisation de passifs | Risques que certains engagements donnés sur passifs soient insuffisamment estimés ou non recensés au bilan | Opérationnel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transac-tion ou dans la gestion des proces-sus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonction nements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30239 | Risques de caution ou assimilés | Risques que les garanties, avals ou cautions ne soient pas suffisamment évalués ou recensés dans les comptes | Opération-nel | | |
| R30301 | Systèmes - Perte ou altération irrémédiable de données informatiques | Perte ou altération irrémédiable de données informatiques (accidentelle) | Opération-nel | | |
| R30302 | Systèmes - Développement | Erreurs de développement | Opération-nel | | |
| R30303 | Systèmes - Sécurité logique | Atteinte involontaire à la sécurité logique | Opération-nel | | |
| R30304 | Systèmes - Ressources informatiques | Inadéquation de ressources informatiques | Opération-nel | | |
| R30305 | Systèmes - Disponibilité des systèmes | Panne système, insuffisance, indisponibilité passagère de ressources informatiques | Opération-nel | | |
| R30306 | Systèmes - Autres causes d'origine technologiques | Autres causes d'origine technologiques (à préciser) | Opération-nel | | |
| R30307 | Systèmes - Disponibilité d'une ressource (énergie, télécommunication) | Défaillance ou indisponibilité d'une ressource (énergie, télécommunication) | Opération-nel | | |
| R30308 | Transports et autres perturbations | Interruption totale ou partielle de l'activité | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R302 | Exécution, Livraison et gestion des processus | Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonctionnements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonctionnements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonctionnements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R303 | Dysfonctionnements de l'activité et des systèmes | Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30309 | Systèmes - Régression | Régression suite à la livraison et la mise en production de nouveaux programmes informatiques ou suite à la mise à jour de programmes ou fonctionnalités existants | Opération-nel | | |
| R30310 | Systèmes - Pérennité | Risques de pérennité de l'outil informatique : correspond à un outil informatique pour lequel la durée de vie est incertaine | Opération-nel | | |
| R30311 | Systèmes - Données | Données informatiques erronées, non conformes aux attentes | Opération-nel | | |
| R30312 | Risques de plan de continuité informatique | Non-continuité de l'exploitation par absence de procédures de secours en cas de difficultés graves dans le fonctionnement des systèmes informatiques | Opération-nel | | |
| R30313 | Systèmes - Recette | Correspond à des tests, jeux d'essais incomplets qui peuvent induire des erreurs plus ou moins graves en production | Opération-nel | | |
| R30401 | Sécurité du lieu de travail - Accidents du travail / maladies professionnelles | Non-respect des règles de santé et de sécurité sur le lieu de travail => accidents du travail / maladies professionnelles | Opération-nel | | |
| R30402 | Sécurité du lieu de travail - Responsabilité civile | Responsabilité civile => accidents de tiers (clients, partenaires, fournisseurs, autres, etc.) | Opération-nel | | |
| R30403 | Relations de travail - Grève, contestation syndicale | Grève, contestation syndicale | Opération-nel | | |
| R30404 | Relations de travail - Litiges avec les employés | Litiges avec les employés / Indemnisation du personnel | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30405 | Egalité et discrimination | Comportement impropre : discrimination / harcèlement | Opération-nel | | |
| R30406 | Gestion des ressources humaines - Recrutements inadaptés | Recrutements inadaptés | Opération-nel | | |
| R30407 | Gestion des ressources humaines - Formation inadaptée | Formation inadaptée | Opération-nel | | |
| R30408 | Gestion des ressources humaines - Gestion des emplois et des compétences | Gestion des emplois et des compétences inadaptée | Opération-nel | | |
| R30409 | Gestion des ressources humaines - Politique sala-riale | Politique salariale inadaptée | Opération-nel | | |
| R30410 | Gestion des ressources humaines - Politique de rémunération et d'évaluation des collaborateurs | Inadaptation de la politique de rémuné-ration variable et d'évaluation annuelle des collaborateurs | Opération-nel | | |
| R30411 | Gestion des ressources humaines - Turnover | Turnover excessif | Opération-nel | | |
| R30412 | Gestion des ressources humaines - Ressource clé | Départ / absence d'une ressource clé | Opération-nel | | |
| R30413 | Gestion des ressources humaines - Protection de la vie privée | Violation des dispositions concernant la protection de la vie privée et des données personnelles des salariés | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompati-bles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompati-bles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompati-bles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompati-bles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R304 | Pratiques en matière d'emploi et de sécurité sur le lieu de travail | Pertes résultant d'actes incompati-bles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30414 | Gestion des ressources humaines - Réglementation sociale | Non-respect de la réglementation sociale (code du travail, conventions collectives, etc.) | Opérationnel | | |
| R30415 | Gestion des ressources humaines - Autre | Autres problèmes liés à la gestion des ressources humaines | Opérationnel | | |
| R30416 | Risques relatifs aux coûts salariaux | Risques d'un niveau de salaire globalement plus élevé que ce qu'il ne devrait être compte tenu de l'état du marché du travail, conduisant à des surcoûts portant préjudice à la compétitivité de l'entreprise | Opérationnel | | |
| R30417 | Risques relatifs aux règles de déontologie | Non-respect par un membre du personnel des règles régissant la profession en matière d'éthique | Opérationnel | | |
| R30418 | Risques relatifs aux règles de déontologie | Non-respect de la déontologie des relations avec un réseau d'apporteurs | Opérationnel | | |
| R30501 | Catastrophes et autres sinistres | Catastrophes et autres sinistres | Opérationnel | | |
| R30502 | Catastrophes et autres sinistres - Autres dommages causés aux actifs corporels | Autres dommages causés aux actifs corporels | Opérationnel | | |
| R30503 | Catastrophes et autres sinistres - Destruction, malveillante de biens | Destruction malveillante de biens / vandalisme | Opérationnel | | |
| R30504 | Catastrophes et autres sinistres - Litiges immeubles et infrastructures | Litiges liés aux immeubles et infrastructures | Opérationnel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R305 | Dommages aux actifs corporels | Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30505 | Catastrophes et autres sinistres - Indisponibilité immeubles et infrastructures | Autres causes liées à l'indisponibilité des immeubles et infrastructures | Opérationnel | | |
| R30506 | Catastrophes et autres sinistres - Pandémie | Pandémie | Opérationnel | | |
| R30507 | Risques générés par les immeubles d'exploitation (en propriété ou en location) | Risques de sinistre (incendie, dommages à des tiers, etc.), risques relatifs à la continuité des opérations, risques relatifs à la gestion des immeubles (hors sécurité du personnel) | Opérationnel | | |
| R30601 | Activité non autorisée - Dissimulation volontaire de position | Dissimulation volontaire de position | Opérationnel | | |
| R30602 | Activité non autorisée - Transactions non notifiées | Transactions intentionnellement non notifiées | Opérationnel | | |
| R30603 | Activité non autorisée - Abus de pouvoir | Abus de pouvoir, activité intentionnelle non autorisée | Opérationnel | | |
| R30604 | Activité non autorisée - Fausses déclarations | Fausses déclarations intentionnelles | Opérationnel | | |
| R30606 | Vol et fraude - Vol / détournement de fonds | Vol / détournement de fonds | Opérationnel | | |
| R30607 | Vol et fraude - Vol / détournement de biens | Vol / détournement de biens | Opérationnel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R306 | Fraude interne | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30608 | Vol et fraude - Contrefaçon de documents | Contrefaçon de documents | Opération-nel | | |
| R30609 | Vol et fraude - Usurpation de compte / d'identité | Usurpation de compte / d'identité | Opération-nel | | |
| R30610 | Vol et fraude - Fraude fiscale | Fraude fiscale / évasion délibérée | Opération-nel | | |
| R30605 | Vol et fraude - Autre | Autres fraudes internes | Opération-nel | | |
| R30611 | Vol et fraude - Délits d'initiés | Non-respect des règles en matière d'opérations financières personnelles / délits d'initiés | Opération-nel | | |
| R30612 | Vol et fraude - Cadeaux et invitations | Non-respect des règles déontologiques relatives aux cadeaux et aux invitations | Opération-nel | | |
| R30613 | Sécurité des systèmes - Malveillance informatique | Malveillance informatique (virus, destruction de fichiers, piratages, etc.) | Opération-nel | | |
| R30614 | Sécurité des systèmes - Données | Vol et divulgation de données | Opération-nel | | |
| R30615 | Vol et fraude - abus de biens sociaux | Risque de faire usage sciemment de biens, du crédit de la société, ou des pouvoirs possédés par des dirigeants sociaux (droits reconnus par la loi ou les statuts aux dirigeants sociaux) contraire aux intérêts de la société et dans un intérêt personnel, intérêt du dirigeant social, des membres de sa famille, de ses proches. | Opération-nel | | |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R3 | Opération-nels | Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs | R307 | Fraude externe | Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'effractions à la législation ou aux règles par une tierce partie |
| R4 | Stratégiques et environ-nementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environ-nement de l'entreprise et aux risques émergents | R401 | Marché de l'assurance | Risques résultant du comportement des acteurs du marché de l'assu-rance |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R30701 | Vol et fraude - Fausses déclarations | Fausses déclarations intentionnelles | Opérationnel | | |
| R30702 | Vol et fraude - Contrefaçon de documents | Contrefaçon de documents | Opérationnel | | |
| R30703 | Vol et fraude - Vol | Vol | Opérationnel | | |
| R30704 | Vol et fraude - Autre | Autres fraudes externes | Opérationnel | | |
| R30705 | Vol et fraude - Usurpation de compte / d'identité | Usurpation de compte / d'identité | Opérationnel | | |
| R30706 | Sécurité des systèmes - Malveillance informatique | Malveillance informatique (virus, destruction de fichiers, piratages, etc.) | Opérationnel | | |
| R30707 | Sécurité des systèmes - Données | Vol et divulgation de données | Opérationnel | | |
| R30708 | Risques de corruption | Risques de corruption active ou passive de membres du personnel, de commerciaux mandataires, salariés ou indépendants (courtiers) | Opérationnel | | |
| R40101 | Risques relatifs aux cycles tarifaires | Risques résultant de la pression du marché à pratiquer des taux tarifaires bas (cyclique en général) | | | Stratégique |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R401 | Marché de l'assurance | Risques résultant du comportement des acteurs du marché de l'assurance |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R402 | Pilotage | Risques de choix stratégiques, de moyens associés ou de pilotage de la mise en oeuvre inadéquats |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R402 | Pilotage | Risques de choix stratégiques, de moyens associés ou de pilotage de la mise en oeuvre inadéquats |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R402 | Pilotage | Risques de choix stratégiques, de moyens associés ou de pilotage de la mise en oeuvre inadéquats |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R403 | Marketing | Risques résultant d'une mauvaise démarche marketing assurance |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R403 | Marketing | Risques résultant d'une mauvaise démarche marketing assurance |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R404 | Organisation | Risques résultant de défauts dans l'organisation de l'entreprise et de ses procédures |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R405 | Réputation | Risques liés à une perception négative de l'entreprise |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R405 | Réputation | Risques liés à une perception négative de l'entreprise |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R40102 | Risques de concurrence | Risques résultant de l'exercice d'activités similaires par d'autres entreprises | | | Stratégique |
| R40201 | Risques sur la mise en oeuvre de la stratégie | Décalage entre la stratégie définie et sa mise en oeuvre, du fait d'erreurs d'appréciation ou de non-adéquation des moyens | | | Stratégique |
| R40202 | Risques relatifs au pilotage stratégique des activités et des filiales | Risques provenant de déficiences du pilotage | | | Stratégique |
| R40203 | Risque de dérive des coûts | Risque de dérive des coûts pour des postes très importants comme le personnel, les immeubles, les systèmes d'information | | | Stratégique |
| R40301 | Risques de mauvaise analyse des marchés cibles | Risques provenant d'une mauvaise identification des besoins, d'une mauvaise segmentation clientèle, etc., conduisant à l'élaboration de produits inadaptés | | | Stratégique |
| R40302 | Risques d'erreur de communication marketing | Décalage entre le contenu d'un message et sa compréhension, ou sa prise en compte, par le destinaire de l'information, et risques de publicité trompeuse | | | Stratégique |
| R40101 | Risques d'inadéquation de l'organisation fonctionnelle | Risques d'inadéquation de l'organisation fonctionnelle aux activités, à la mise en oeuvre de la stratégie, au profil des compétences disponibles, à la gestion des relations avec les intermédiaires et avec les clients, etc. | | | Stratégique |
| R40501 | Risques d'image du secteur de l'assurance | Risques résultant de la mise en cause publique de pratiques particulières d'une ou plusieurs compagnies (hors entente), ou d'erreurs de communication publique | | | Réputation |
| R40502 | Risques d'image - Risques provenant d'un manquement aux règles de bonne conduite | Risques provenant d'un manquement aux règles de bonne conduite, aux normes professionnelles ou aux valeurs de la société | | | Réputation |



© IFACI

| Niveau 1 | Famille | Définition Risques Niveau 1 | Niveau 2 | Risques Niveau 2 | Définition Risques Niveau 2 |
|---|---|---|---|---|---|
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R405 | Réputation | Risques liés à une perception négative de l'entreprise |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R405 | Réputation | Risques liés à une perception négative de l'entreprise |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R405 | Réputation | Risques liés à une perception négative de l'entreprise |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R406 | Législatifs, réglementaires et judiciaires | Risques liés à l'apparition de nouvelles lois ou réglements, et à leur application |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R407 | Autres risques systémiques et exogènes | Autres risques provenant de l'environnement externe de l'entreprise |
| R4 | Stratégiques et environnementaux | Risques relatifs au pilotage de l'entreprise, aux risques de réputation directe et aux risques générés par l'environnement de l'entreprise et aux risques émergents | R407 | Autres risques systémiques et exogènes | Autres risques provenant de l'environnement externe de l'entreprise |





© IFACI

| Niveau 3 | Risques Niveau 3 | Définition Risques Niveau 3 | Catégorie S2 | | |
|---|---|---|---|---|---|
| | | | Module de risque | Sous module de risque | Autres |
| R40503 | Risques d'image - Risques juridiques et de mise en cause | Risques de mise en cause judiciaire ou non, par une association de consommateurs, par la presse, ou par un client important, de litige sur l'application d'un contrat | | | Stratégique |
| R40504 | Risques d'image - Risques de communication externe | Politique de communication sur l'identité de l'entreprise inadéquate au marché, aux intermédiaires, aux interlocuteurs financiers ou institutionnels, etc. | | | Réputation |
| R40505 | Risques d'image - Risques liés aux médias sociaux | Risques liés aux médias sociaux qui affectent à court, moyen ou long terme la confiance envers un organisme d'assurance | | | Réputation |
| R40601 | Législatifs, réglementaires et judiciaires | Risques liés à l'apparition de nouvelles lois ou réglements, et à leur application | | | Réputation |
| R40701 | Risques économiques | Risques d'inflation, de dépression, d'évolution de la demande | | | Stratégique |
| R40702 | Risques politiques | Risques de guerre civile, d'émeutes, de guerre étrangère, d'attentats et de terrorisme | | | Risques externes |



© IFACI

| Étiquettes de lignes | Nombre de Risques Niveau 3 |
|---|---|
| **Assurances** | **22** |
| Maitrîse des Résultats | 1 |
| Participations aux bénéfices | 1 |
| Provisionnement | 3 |
| Réassurance de protection | 3 |
| Sinistralité non vie / Prestations vie | 5 |
| Souscription | 6 |
| Technique | 3 |
| **Financiers** | **26** |
| Adéquation Actif/Passif | 8 |
| Endettement | 2 |
| Gestion d'actifs | 13 |
| Risques de solvabilité | 3 |
| **Opérationnels** | **128** |
| Clients / tiers, produits et pratiques commerciales | 28 |
| Dommages aux actifs corporels | 7 |
| Dysfonctionnements de l'activité et des systèmes | 13 |
| Exécution, Livraison et gestion des processus | 39 |
| Fraude externe | 8 |
| Fraude interne | 15 |
| Pratiques en matière d'emploi et de sécurité sur le lieu de travail | 18 |
| **Stratégiques et environnementals** | **16** |
| Autres risques systémiques et exogènes | 2 |
| Législatifs, réglementaires et judiciaires | 1 |
| Marché de l'assurance | 2 |
| Marketing | 2 |
| Organisation | 1 |
| Pilotage | 3 |
| Réputation | 5 |
| **Total général** | **192** |





© IFACI

# ANNEXE 3

## Présentation des risques de la formule standard du calcul du SCR



© IFACI

| N° | Module | Définition | Commentaire |
|---|---|---|---|
| 1 | Risque de marché | Le module « risque de marché » reflète le risque lié au niveau ou à la volatilité de la valeur de marché des instruments financiers ayant un impact sur la valeur des actifs et des passifs de l'entreprise concernée. Il reflète de manière adéquate toute inadéquation structurelle entre les actifs et les passifs, en particulier au regard de leur duration | Le risque de marché résulte du niveau ou de la volatilité des cours de marché des instruments financiers qui ont un impact sur la valeur des actifs et des passifs de l'entreprise concernée. L'exposition au risque de marché est mesurée par l'impact des mouvements dans le niveau des variables financières tel que le cours des actions, les taux d'intérêt, les cours de l'immobilier et les taux de change |



© IFACI

| N° | Sous module | Définition | Commentaire |
|---|---|---|---|
| 1.1 | Risque de taux d'intérêt | Risque lié à la sensibilité de la valeur des actifs, des passifs et des instruments financiers aux changements affectant la courbe des taux d'intérêt ou la volatilité des taux d'intérêt | |
| 1.2 | Risque sur actions | Risque lié à la sensibilité de la valeur des actifs, des passifs et des instruments financiers aux changements affectant le niveau ou la volatilité de la valeur de marché des actions | |
| 1.3 | Risque sur actifs immobiliers | Risque lié à la sensibilité de la valeur des actifs, des passifs et des instruments financiers aux changements affectant le niveau ou la volatilité de la valeur de marché des actifs immobiliers | |
| 1.4 | Risque lié à la marge *(spread)* | Risque lié à la sensibilité de la valeur des actifs, des passifs et des instruments financiers aux changements affectant le niveau ou la volatilité des marges ***(spreads)*** de crédit par rapport à la courbe des taux d'intérêt sans risque | |
| 1.5 | Risque de change | Risque lié à la sensibilité de la valeur des actifs, des passifs et des instruments financiers aux changements affectant le niveau ou la volatilité des taux de change | |
| 1.6 | Concentrations du risque de marché | Risques supplémentaires supportés par l'entreprise d'assurance ou de réassurance du fait soit d'un manque de diversification de son portefeuille d'actifs, soit d'une exposition importante au risque de défaut d'un seul émetteur de valeurs mobilières ou d'un groupe d'émetteurs liés | |
| 1.7 | Contracyclique | | |



© IFACI

| N° | Module | Définition | Commentaire |
|---|---|---|---|
| 2 | Risque de souscription en santé | Le module « risque de souscription en santé » reflète le risque découlant de la souscription d'engagements d'assurance santé, qu'il s'exerce ou non sur une base technique similaire à celle de l'assurance vie, compte tenu des périls couverts et des procédés appliqués dans l'exercice de cette activité | Le risque de souscription Santé couvre le risque de souscription pour toutes les garanties santé et accidents du travail ; il se divise en trois sous modules : santé à long terme pratiquée sur une base similaire à celle de l'assurance vie (qui n'existe qu'en Allemagne et Autriche), santé court terme et accidents du travail. |



© IFACI

| N° | Sous module | Définition | Commentaire |
|---|---|---|---|
| 2.1 | Risque de mortalité | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux de mortalité, lorsqu'une augmentation de ces taux entraîne une augmentation de la valeur des engagements d'assurance | Le risque de mortalité est le risque que les assurés meurent plus vite que ne le prévoyaient les hypothèses initiales. Il s'applique à tous les engagements pour lesquels les prestations à payer en cas de décès excèdent les provisions techniques, et pour lesquels une hausse de la mortalité conduira donc à une augmentation des provisions techniques. |
| 2.2 | Risque de longévité | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux de mortalité, lorsqu'une baisse de ces taux entraîne une augmentation de la valeur des engagements d'assurance. | Le risque de longévité s'applique aux contrats pour lesquels une baisse de la mortalité conduirait à une hausse des provisions techniques, tels que les contrats de retraite supplémentaire. |
| 2.3 | Risque d'invalidité – de morbidité | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux d'invalidité, de maladie et de morbidité | |
| 2.4 | Risque de rachat | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau ou la volatilité des taux de cessation, d'échéance, de renouvellement et de rachat des polices | |
| 2.5 | Risque de dépenses | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des dépenses encourues pour la gestion des contrats d'assurance ou de réassurance | |
| 2.6 | Risque de révision | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux de révision applicables aux rentes, sous l'effet d'un changement de l'environnement juridique ou de l'état de santé de la personne assurée | |
| 2.7 | Risque de catastrophe en santé | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de l'incertitude importante, liée aux épidémies majeures et à l'accumulation inhabituelle de risques qui se produit dans ces circonstances extrêmes, qui pèse sur les hypothèses retenues en matière de prix et de provisionnement | |
| 2.8 | Risque de primes et de réserve en santé | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant la date de survenance, la fréquence et la gravité des événements assurés, ainsi que la date et le montant des règlements de sinistres au moment du provisionnement | Dans sous module NSLT : pratiqué en Allemagne et Autriche |



© IFACI

| N° | Module | Définition | Commentaire |
|---|---|---|---|
| 3 | Risque de défaut ou de contrepartie | Le module « risque de contrepartie » reflète les pertes possibles que pourrait entraîner le défaut inattendu, ou la détérioration de la qualité de crédit, des contreparties et débiteurs de l'entreprise d'assurance ou de réassurance durant les douze mois à venir. Le module « risque de contrepartie » couvre les contrats d'atténuation des risques, tels que les accords de réassurance, les titrisations et les instruments dérivés, et les paiements à recevoir des intermédiaires ainsi que tout autre risque de crédit ne relevant pas du sous-module « risque lié à la marge ». Il prend en compte, de manière appropriée, les garanties ou autres sûretés détenues par l'entreprise d'assurance ou de réassurance ou pour son compte, et les risques qui y sont liés. | Le risque de défaut ou de contrepartie représente le risque qu'un débiteur ou une contrepartie de la société d'assurance ou de réassurance n'honore pas ses engagements dans les conditions initialement prévues. |
| 4 | Risque de souscription en vie | Le module « risque de souscription en vie » reflète le risque découlant des engagements d'assurance vie, compte tenu des périls couverts et des procédés appliqués dans l'exercice de cette activité. | Le risque de souscription Vie regroupe l'ensemble des risques lié à une tarification insuffisamment prudente lors de la souscription ou le rachat du contrat (comprenant le risque de mortalité, de longévité, de rachat, etc.). |





© IFACI

| N° | Sous module | Définition | Commentaire |
|---|---|---|---|
| | | | |
| 4.1 | Risque de mortalité | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux de mortalité, lorsqu'une augmentation de ces taux entraîne une augmentation de la valeur des engagements d'assurance | |
| 4.2 | Risque de longévité | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux de mortalité, lorsqu'une baisse de ces taux entraîne une augmentation de la valeur des engagements d'assurance. | |
| 4.3 | Risque d'invalidité – de morbidité | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux d'invalidité, de maladie et de morbidité | |
| 4.4 | Risque de dépenses en vie | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des dépenses encourues pour la gestion des contrats d'assurance ou de réassurance. | |
| 4.5 | Risque de révision | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau, l'évolution tendancielle ou la volatilité des taux de révision applicables aux rentes, sous l'effet d'un changement de l'environnement juridique ou de l'état de santé de la personne assurée | |
| 4.6 | Risque de rachat | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau ou la volatilité des taux de cessation, d'échéance, de renouvellement et de rachat des polices | |
| 4.7 | Risque de catastrophe en vie | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de l'incertitude importante, liée aux événements extrêmes ou irréguliers, qui pèse sur les hypothèses retenues en matière de prix et de provisionnement | |



© IFACI

| N° | Module | Définition | Commentaire |
|---|---|---|---|
| 5 | Risque de souscription en non-vie | Le module «risque de souscription en non-vie» reflète le risque découlant des engagements d'assurance non-vie, compte tenu des périls couverts et des procédés appliqués dans l'exercice de cette activité. Il tient compte de l'incertitude pesant sur les résultats des entreprises d'assurance et de réassurance dans le cadre de leurs engagements d'assurance et de réassurance existants, ainsi que du nouveau portefeuille dont la souscription est attendue dans les douze mois à venir. | Le risque de souscription Non vie représente le risque d'assurance spécifique résultant des contrats d'assurance. Il fait référence à l'incertitude concernant les résultats de la souscription de l'assureur (montants et délais de règlements des sinistres, taux de primes nécessaires pour couvrir les passifs, etc.). |
| 6 | Risque sur actifs incorporels | Risque de perte, ou de changement défavorable de la situation financière, résultant de fluctuations affectant le niveau ou la volatilité de la valeur des actifs incorporels (logiciels, brevets, marques, etc.) présents au bilan de l'organisme d'assurance. | Le risque d'actifs incorporels porte sur les actifs incorporels qui sont exposés à deux types de risques : le risque de marché et le risque interne inhérent à la nature même de ces éléments. Les actifs incorporels représentent les actifs immatériels de l'entreprise tels que le "*goodwill*", les brevets, les licences, les marques, |
| 7 | Risque opérationnel | Le risque opérationnel est le risque de perte résultant de procédures internes inadaptées ou défaillantes, du personnel, des systèmes ou d'événements extérieurs. Il comprend également les risques juridiques, mais il exclut les risques de réputation et les risques résultant de décisions stratégiques. Le module Risque opérationnel tient compte des risques opérationnels non explicitement couverts dans d'autres modules de risque. Le besoin en capital pour couvrir le risque opérationnel est calculé de façon forfaitaire. | |





© IFACI

| N° | Sous module | Définition | Commentaire |
|---|---|---|---|
| 5.1 | Risque de primes et de réserve en non-vie | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant la date de survenance, la fréquence et la gravité des événements assurés, ainsi que la date et le montant des règlements de sinistres | |
| 5.2 | Risque de catastrophe en non-vie | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de l'incertitude importante, liée aux événements extrêmes ou exceptionnels, qui pèse sur les hypothèses retenues en matière de prix et de provisionnement. | |
| 5.3 | Risque de rachat | Risque de perte, ou de changement défavorable de la valeur des engagements d'assurance, résultant de fluctuations affectant le niveau ou la volatilité des taux de cessation, d'échéance, de renouvellement et de rachat des polices | |
| | | | |
| | | | |



© IFACI

# ANNEXE 4

## Exemple d'impact financier

| Type d'effets | Description |
|---|---|
| Dépréciation (Write-down) | Dépréciation d'actifs dans les comptes suite à un événement de risque opérationnel.<br>Par exemple : Vol au sein de la société, fraude interne ou externe, erreur tarifaire aboutissant à un revers inférieur aux prévisions. |
| Dédommagements (Compensation) | Paiements à des tiers suite à des événements opérationnels dont la société est légalement responsable.<br>Par exemple : Réclamations de clients suite à un arrêt d'activité de la société ou des erreurs tarifaires, intérêts versés suite à un retard dans un paiement, fraude de salarié sur compte client.<br>Cela n'inclut pas la réduction du propre revenu de la société en raison d'un arrêt d'activité, les pertes résultant d'une atteinte à la réputation de la société. |
| Pertes de recours (Loss of Recourse) | Pertes résultant de l'incapacité de la société à mettre en œuvre des réclamations / recours auprès d'un tiers. La perte peut être encourue quand un tiers ne respecte pas ou ne peut pas respecter ses obligations, causées par un événement opérationnel.<br>Par exemple : Un double paiement fait à un tiers qui ne peut pas être récupéré. |
| Responsabilités juridiques (Legal Liability) | Frais encourus dans le cadre de litiges, de procès (y compris frais d'avocat, règlements judiciaires, condamnations).<br>Par exemple : Règlements à l'amiable, coûts juridiques et autres dépenses y afférentes.<br>Cela n'inclut pas les coûts relatifs à l'amélioration de la documentation ou des traitements. |
| Actions réglementaires (Regulatory Action) | Amendes ou règlements imposés par les autorités / organismes réglementaires à la suite d'actions non conformes faites par la société.<br>Par exemple : Amendes versées pour régler des contraventions à la réglementation, etc.<br>Cela ne comprend pas la perte de revenu suite à la révocation d'une licence, les honoraires d'avocat, etc., de recherche d'un changement d'une disposition réglementaire qui serait favorable à l'entreprise. |
| Dépenses fiscales (Tax Expenses) | Pertes encourues en raison de paiements d'impôts supplémentaires auxquels la société doit faire face.<br>Par exemple : Pénalités fiscales ou taxes supplémentaires |
| Pertes ou dommages sur des actifs (Loss / Damage to Physical Asset) | Dépréciation des actifs corporels en raison de la survenance d'un événement opérationnel (négligence, incendie, accident, tremblement de terre).<br>Par exemple : Coûts de remplacement du matériel volé ou endommagé, coût de la reprise immédiate d'activités, coûts associés aux réparations à des actifs ; pertes de biens incorporels (données, etc.).<br>Cela n'inclut pas les améliorations apportées au cours de la reconstruction après un incendie, une inondation ou une catastrophe naturelle (améliorations par rapport à la situation initiale avant l'événement). |
| Autres coûts ou pertes (Other Losses and/or Costs) | Pertes et/ou coûts non concernés par les natures précédentes.<br>Par exemple : Coût des consultants externes / personnel temporaire pour enquêter ou résoudre le problème, les coûts de reproduction ou de remplacement, etc.<br>Cela n'inclut pas le temps consacré à l'analyse et la résolution de problèmes, les coûts de support interne (support informatique, audit interne), l'amélioration des contrôles de prévention, baisse de revenus en raison d'un impact sur la réputation. |





© IFACI

# ANNEXE 5

## Evaluation de l'impact financier d'un incident

### *Exemples d'événement et leur retranscription en termes d'impact financier*

1) *Passation par pertes et profits de valeurs immobilisées suite à une destruction d'actifs*
   - **Passation en compte de perte et profit** de valeurs immobilisées corporelles suite à une destruction d'actifs, destruction de locaux et matériels suite à un sinistre.
   - **Coût externe de remise en l'état** de valeurs immobilisées suite à une dégradation.
   - **Passation en compte de perte et profit** de valeurs immobilisées incorporelles suite à l'abandon d'un projet informatique.
   - **Coût d'achat ou de remise en l'état** de biens non immobilisés suite à une destruction ou un vol.

2) *Diminution d'actifs due à la fraude, au vol ou à une erreur d'exécution*
   - **Diminution d'actifs** due au vol, à la fraude, aux activités non autorisées, aux pertes de marché.
   - **Passation en compte de perte et profit** de suspens comptables résultant de la survenance d'un risque opérationnel.

3) *Perte sèche due à une sortie de fonds non récupérée*
   - **Fonds transférés par erreur, virements réalisés en double** et non récupérés auprès du bénéficiaire.
   - **Charges externes supplémentaires :**
     - coût de relogement temporaire des activités suite à un sinistre,
     - recours à des intérimaires ou prestataires externes en situation de crise ou pour résoudre des problèmes suite à des défaillances.

4) *Perte sèche liée à la compensation de tiers en cas d'erreur imputable à l'organisme d'assurance*
   - **Indemnisation du client ou intérêts de retard** versés à une contrepartie, y compris les avoirs sur factures et commissions.
   - **Indemnisation et prises en charge** en cas de responsabilité de l'organisme d'assurance sans qu'il soit en faute : indemnisation du personnel en cas d'accident.



© IFACI

*5) Condamnation à payer et autres frais juridiques*

- **Condamnation à payer** et autres dommages et intérêts attachés à une procédure judiciaire.
- **Coûts juridiques** attachés à la procédure judiciaire (honoraires d'avocat, etc.).

*6) Pénalité ou amende réglementaire ou fiscale*

- **Pénalité ou amende** réglementaire ou fiscale à payer.
- **Intérêts de retard fiscaux** à payer, dans tous les cas, que l'entreprise se considère défaillante ou non (événement externe).
- **Redressement fiscal** correspondant à l'impôt qui aurait dû être payé (TIMING IMPACT).

*7) Autres coûts de trésorerie*

- **Coûts de trésorerie** lorsqu'ils permettent de traduire l'effet d'une crise majeure et fondent une demande d'indemnisation (erreur dans les transferts de fonds, erreur dans les livraisons de titres, erreur dans la mise en place de couvertures, etc.).
- **Augmentation des frais généraux :**
  - coûts de communication pour résolution de crise,
  - coûts de reconstitution, réédition, réexpédition de documents.
- **Heures supplémentaires internes et astreintes** consacrées à la résolution d'incidents relevant du risque opérationnel.

*8) Surcoût interne de réparation*

- **Temps** passé par le personnel affecté à la résolution de dysfonctionnements dans le cadre de l'horaire légal (coût standard).
- **Surcoût interne lié à l'inactivité :** heures non travaillées dues à l'indisponibilité des locaux ou postes de travail.

*9) Conséquence positive d'une erreur*

- **Dénouement positif** d'une erreur de bourse suite à une évolution favorable des cours.

***Autres cas***

- **Manque à gagner** (non objectivement vérifiable) correspondant à la perte d'opportunités commerciales liée à la suspension temporaire d'activité (sanction ou inaccessibilité du site).
- **Manque à gagner** correspondant à une perte de chiffre d'affaires récurrent, donc prévisible et objectivement vérifiable suite à une défaillance des systèmes d'information ou à un sinistre.
  Exemple : panne prolongée ou répétée des applicatifs de souscription.





© IFACI

- **Manque à gagner** correspondant à des commissions dues mais non perçues (défaut dans le processus de facturation ou de recouvrement)
- **Incident évité en l'absence de contrôle et sans conséquence financière** (voir section 3.2.1 sur les quasi-pertes / *near misses*) :
  - Erreur rattrapée dans des délais suffisants pour ne pas engendrer de pénalités ;
  - Sommes versées par erreur mais récupérées dans les meilleurs délais ;
  - Fraude déjouée.
- **Geste commercial** ne venant pas compenser une erreur de l'organisme d'assurance.
- **Dépassement de budget** de projets.



© IFACI

# ANNEXE 6

## Illustration – Synthèse du processus de collecte des événements

| Processus | Tâches | Acteurs | |
|---|---|---|---|
| Identification des événements | • Notification de l'événement<br>• Description de l'événement et de la cause<br>• Estimation des conséquences financières<br>• Définition de la catégorie du risque lié | Déclarant | Services opérationnels |
| Enregistrement et validation des événements (niveau 1) | • Analyse des cas déclarés<br>• Enregistrement dans la base des événements / impacts éligibles à la collecte | Loss identifier | Contrôle interne<br>Contrôle permanent |
| | • Vérification complétude et qualité<br>• Validation de la cohérence | Loss Assessor (superviseur) | |
| Validation des événements (niveau 2) | • Consolidation des données<br>• Validation des événements déclarés<br>• Analyse et diffusion des données | Loss Approver (valideur) | Direction des risques |





© IFACI

# ANNEXE 7

## Directive *Solvabilité II* (extraits)

Directive du parlement européen et du conseil sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II). Version consolidée du 25 novembre 2009.

### *Article 13 - Définitions*

30. « risque de souscription » : le risque de perte ou de changement défavorable de la valeur des engagements d'assurance, en raison d'hypothèses inadéquates en matière de tarification et de provisionnement ;

31. « risque de marché » : le risque de perte, ou de changement défavorable de la situation financière, résultant, directement ou indirectement, de fluctuations affectant le niveau et la volatilité de la valeur de marché des actifs, des passifs et des instruments financiers ;

32. « risque de crédit » : le risque de perte, ou de changement défavorable de la situation financière, résultant de fluctuations affectant la qualité de crédit d'émetteurs de valeurs mobilières, de contreparties ou de tout débiteur, auquel les entreprises d'assurance et de réassurance sont exposées sous forme de risque de contrepartie, de risque lié à la marge ou de concentration du risque de marché ;

33. « risque opérationnel » : le risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs ;

34. « risque de liquidité » : le risque, pour les entreprises d'assurance et de réassurance, de ne pas pouvoir réaliser leurs investissements et autres actifs en vue d'honorer leurs engagements financiers au moment où ceux-ci deviennent exigibles ;

35. « risque de concentration » : toutes les expositions au risque qui sont assorties d'un potentiel de perte suffisamment important pour menacer la solvabilité ou la situation financière des entreprises d'assurance et de réassurance.

### *Article 41 - Exigences générales en matière de gouvernance*

1. Les États membres exigent de toutes les entreprises d'assurance et de réassurance qu'elles mettent en place un système de gouvernance efficace, qui garantisse une gestion saine et prudente de l'activité.



© IFACI

Ce système comprend au moins une structure organisationnelle transparente adéquate, avec une répartition claire et une séparation appropriée des responsabilités, ainsi qu'un dispositif efficace de transmission des informations. Il satisfait aux exigences énoncées aux articles 42 à 49.
Le système de gouvernance fait l'objet d'un réexamen interne régulier.

2. Le système de gouvernance est proportionné à la nature, à l'ampleur et à la complexité des opérations de l'entreprise d'assurance ou de réassurance.

3. Les entreprises d'assurance et de réassurance disposent de politiques écrites concernant au moins leur gestion des risques, leur contrôle interne, leur audit interne et, le cas échéant, la sous-traitance. Elles veillent à ce que ces politiques soient mises en œuvre.
Ces politiques écrites sont réexaminées au moins une fois par an. Elles sont soumises à l'approbation préalable de l'organe d'administration, de gestion ou de contrôle et elles sont adaptées compte tenu de tout changement important affectant le système ou le domaine concerné.

4. Les entreprises d'assurance et de réassurance prennent des mesures raisonnables afin de veiller à la continuité et à la régularité dans l'accomplissement de leurs activités, y compris par l'élaboration de plans d'urgence. À cette fin, elles utilisent des systèmes, des ressources et des procédures appropriés et proportionnés.

5. Les autorités de contrôle disposent des moyens, méthodes et pouvoirs appropriés pour vérifier le système de gouvernance des entreprises d'assurance et de réassurance et pour évaluer les risques émergents détectés par ces entreprises et susceptibles d'affecter leur solidité financière.
Les États membres veillent à ce que les autorités de contrôle disposent des pouvoirs nécessaires pour exiger que le système de gouvernance soit amélioré et renforcé de façon à satisfaire aux exigences énoncées aux articles 42 à 49.

### *Article 44 - Gestion des risques.*

1. Les entreprises d'assurance et de réassurance mettent en place un système de gestion des risques efficace, qui comprenne les stratégies, processus et procédures d'information nécessaires pour déceler, mesurer, contrôler, gérer et déclarer, en permanence, les risques, aux niveaux individuel et agrégé, auxquels elles sont ou pourraient être exposées ainsi que les interdépendances entre ces risques. Ce système de gestion des risques est efficace, parfaitement intégré à la structure organisationnelle et aux procédures de prise de décision de l'entreprise d'assurance ou de réassurance et dûment pris en compte par les personnes qui dirigent effectivement l'entreprise ou qui occupent d'autres fonctions clés.





© IFACI

2. Le système de gestion des risques couvre les risques à prendre en considération dans le calcul du capital de solvabilité requis conformément à l'article 101, paragraphe 4, ainsi que les risques n'entrant pas ou n'entrant pas pleinement dans ce calcul.
   Le système de gestion des risques couvre au moins les domaines suivants :
   a) la souscription et le provisionnement ;
   b) la gestion actif-passif ;
   c) les investissements, en particulier dans les instruments dérivés et engagements similaires ;
   d) la gestion du risque de liquidité et de concentration ;
   e) la gestion du risque opérationnel ;
   f) la réassurance et les autres techniques d'atténuation du risque.

   Les politiques écrites concernant la gestion des risques visées à l'article 41, paragraphe 3, comprennent des politiques concernant le deuxième alinéa, points a) à f), du présent paragraphe.

3. En ce qui concerne le risque d'investissement, les entreprises d'assurance et de réassurance démontrent qu'elles satisfont aux dispositions du chapitre VI, section 6.

4. Les entreprises d'assurance et de réassurance prévoient une fonction de gestion des risques, qui est structurée de façon à faciliter la mise en œuvre du système de gestion des risques.

5. Pour les entreprises d'assurance et de réassurance utilisant un modèle interne partiel ou intégral qui a été approuvé conformément aux articles 112 et 113, la fonction de gestion des risques recouvre les tâches supplémentaires suivantes :
   a) conception et mise en œuvre du modèle interne ;
   b) test et validation du modèle interne ;
   c) suivi documentaire du modèle interne et de toute modification qui lui est apportée ;
   d) analyse de la performance du modèle interne et production de rapports de synthèse concernant cette analyse ;
   e) information de l'organe d'administration, de gestion ou de contrôle concernant la performance du modèle interne en suggérant des éléments à améliorer, et communication à cet organe de l'état d'avancement des efforts déployés pour remédier aux faiblesses précédemment détectées.

### *Article 45 - Évaluation interne des risques et de la solvabilité*

1. Dans le cadre de son système de gestion des risques, chaque entreprise d'assurance et de réassurance procède à une évaluation interne des risques et de la solvabilité.



© IFACI

Cette évaluation porte au moins sur les éléments suivants :

a) le besoin global de solvabilité, compte tenu du profil de risque spécifique, des limites approuvées de tolérance au risque et de la stratégie commerciale de l'entreprise ;

b) le respect permanent des exigences de capital prévues au chapitre VI, sections 4 et 5, et des exigences concernant les provisions techniques prévues au chapitre VI, section 2 ;

c) la mesure dans laquelle le profil de risque de l'entreprise s'écarte des hypothèses qui sous-tendent le capital de solvabilité requis prévu à l'article 101, paragraphe 3,calculé à l'aide de la formule standard conformément au chapitre VI, section 4, sous-section 2, ou avec un modèle interne partiel ou intégral conformément au chapitre VI, section 4, sous-section 3.

2. Aux fins du paragraphe 1, point a), l'entreprise concernée met en place des procédures qui sont proportionnées à la nature, à l'ampleur et à la complexité des risques inhérents à son activité et qui lui permettent d'identifier et d'évaluer de manière adéquate les risques auxquels elle est exposée à court et long terme, ainsi que ceux auxquels elle est exposée, ou pourrait être exposée. L'entreprise démontre la pertinence des méthodes qu'elle utilise pour cette évaluation.

3. Dans le cas visé au paragraphe 1, point c), lorsqu'un modèle interne est utilisé, l'évaluation est effectuée parallèlement au recalibrage qui aligne les résultats du modèle interne sur la mesure de risque et le calibrage qui sous-tendent le capital de solvabilité requis.

4. L'évaluation interne des risques et de la solvabilité fait partie intégrante de la stratégie commerciale et il en est tenu systématiquement compte dans les décisions stratégiques de l'entreprise.

5. Les entreprises d'assurance et de réassurance procèdent à l'évaluation visée au paragraphe 1 sur une base régulière et immédiatement à la suite de toute évolution notable de leur profil de risque.

6. Les entreprises d'assurance et de réassurance informent les autorités de contrôle des conclusions de chaque évaluation interne des risques et de la solvabilité, dans le cadre des informations à fournir en vertu de l'article 35.

7. L'évaluation interne des risques et de la solvabilité ne sert pas à calculer un montant de capital requis. Le capital de solvabilité requis n'est ajusté que conformément aux articles 37, 231 à 233 et 238.





© IFACI

# ANNEXE 8

## Décret n·2006-287 du 13 mars 2006 relatif au contrôle interne des entreprises d'assurance et modifiant le Code des assurances (extraits)

Les entreprises d'assurance doivent rendre compte dans une première partie des conditions de préparation et d'organisation des travaux du Conseil de surveillance, et dans une seconde partie les procédures de contrôle interne mises en place.

La seconde partie de ce rapport détaille donc :

a) Les objectifs, la méthodologie, la position et l'organisation générale du contrôle interne au sein de l'entreprise ; les mesures prises pour assurer l'indépendance et l'efficacité du contrôle interne et notamment la compétence et l'expérience des équipes chargées de le mettre en œuvre, ainsi que les suites données aux recommandations des personnes ou instances chargées du contrôle interne ;

b) Les procédures permettant de vérifier que les activités de l'entreprise sont menées selon les politiques et stratégies établies par les organes dirigeants et les procédures permettant de vérifier la conformité des opérations d'assurance aux dispositions législatives et réglementaires ;

c) Les méthodes utilisées pour assurer la mesure, l'évaluation et le contrôle des placements, en particulier en ce qui concerne l'évaluation de la qualité des actifs et de la gestion actif-passif, le suivi des opérations sur instruments financiers à terme et l'appréciation des performances et des marges des intermédiaires financiers utilisés ;

d) Le dispositif interne de contrôle de la gestion des placements, ce qui inclut la répartition interne des responsabilités au sein du personnel, les personnes chargées d'effectuer les transactions ne pouvant être également chargées de leur suivi, les délégations de pouvoir, la diffusion de l'information, les procédures internes de contrôle ou d'audit ;

e) Les procédures et dispositifs permettant d'identifier, d'évaluer, de gérer et de contrôler les risques liés aux engagements de l'entreprise et de détenir des capitaux suffisants pour ces risques, ainsi que les méthodes utilisées pour vérifier la conformité des pratiques en matière d'acceptation et de tarification du risque, de cession en réassurance et de provisionnement des engagements réglementés à la politique de l'entreprise dans ces domaines, définie dans les rapports mentionnés à l'article L. 322-2-4 et à l'article R. 336-5 ;

f) Les mesures prises pour assurer le suivi de la gestion des sinistres, le suivi des filiales, la maîtrise des activités externalisées et des modes de commercialisation des produits de l'entreprise, et les risques qui pourraient en résulter ;

g) Les procédures d'élaboration et de vérification de l'information financière.

*Décret n° 2006-287 du 13 mars 2006 relatif au contrôle interne des entreprises d'assurance et modifiant le code des assurances (partie réglementaire)*



© IFACI

# ANNEXE 9

## Décret n°2008-468 du 19 mai 2008 relatif au contrôle interne des institutions de prévoyance, des mutuelles et de leurs unions

Art. R. 931-43.- L'institution ou l'union est tenue de mettre en place un dispositif permanent de contrôle interne. « Le conseil d'administration approuve, au moins annuellement, un rapport sur le contrôle interne, qui est transmis à l'Autorité de contrôle des assurances et des mutuelles.

« 1° La première partie de ce rapport détaille les conditions de préparation et d'organisation des travaux du conseil d'administration et, le cas échéant, les pouvoirs nécessaires à la gestion de l'institution ou de l'union délégués au directeur général par le conseil d'administration dans le cadre de l'article R. 931-3-11.

«2° La seconde partie de ce rapport détaille :

« a) Les objectifs, la méthodologie, la position et l'organisation générale du contrôle interne au sein de l'institution ou de l'union ; les mesures prises pour assurer l'indépendance et l'efficacité du contrôle interne et notamment la compétence et l'expérience des équipes chargées de le mettre en œuvre, ainsi que les suites données aux recommandations des personnes ou instances chargées du contrôle interne ;

« b) Les procédures permettant de vérifier que les activités de l'institution ou de l'union sont conduites selon les politiques et stratégies établies par les organes dirigeants et les procédures permettant de vérifier la conformité des opérations d'assurance aux dispositions législatives et réglementaires ;

« c) Les méthodes utilisées pour assurer la mesure, l'évaluation et le contrôle des placements, en particulier en ce qui concerne l'évaluation de la qualité des actifs et de la gestion actif-passif, le suivi des opérations sur instruments financiers à terme et l'appréciation des performances et des marges des intermédiaires financiers utilisés ;

« d) Le dispositif interne de contrôle de la gestion des placements, ce qui inclut la répartition interne des responsabilités au sein du personnel, les personnes chargées d'effectuer les transactions ne pouvant être également chargées de leur suivi, les délégations de pouvoir, la diffusion de l'information, les procédures internes de contrôle ou d'audit ;

« e) Les procédures et dispositifs permettant d'identifier, d'évaluer, de gérer et de contrôler les risques liés aux engagements de l'institution ou de l'union et de détenir des capitaux suffisants pour ces risques, ainsi que les méthodes utilisées pour vérifier la conformité des pratiques en matière d'acceptation et de tarification du risque, de cession en réassurance et de provisionnement des engagements réglementés à la politique de l'institution ou de l'union dans ces domaines, définie dans le rapport mentionné à l'article L. 322-2-4 du code des assurances ;





© IFACI

« f) Les mesures prises pour assurer le suivi de la gestion des sinistres, le suivi des filiales, la maîtrise des activités externalisées et des modes de commercialisation des produits de l'institution ou de l'union, et les risques qui pourraient en résulter ;
« g) Les procédures d'élaboration et de vérification de l'information financière et comptable.

*Décret n° 2008-468 du 19 mai 2008 relatif au contrôle interne des institutions de prévoyance, des mutuelles et de leurs unions*



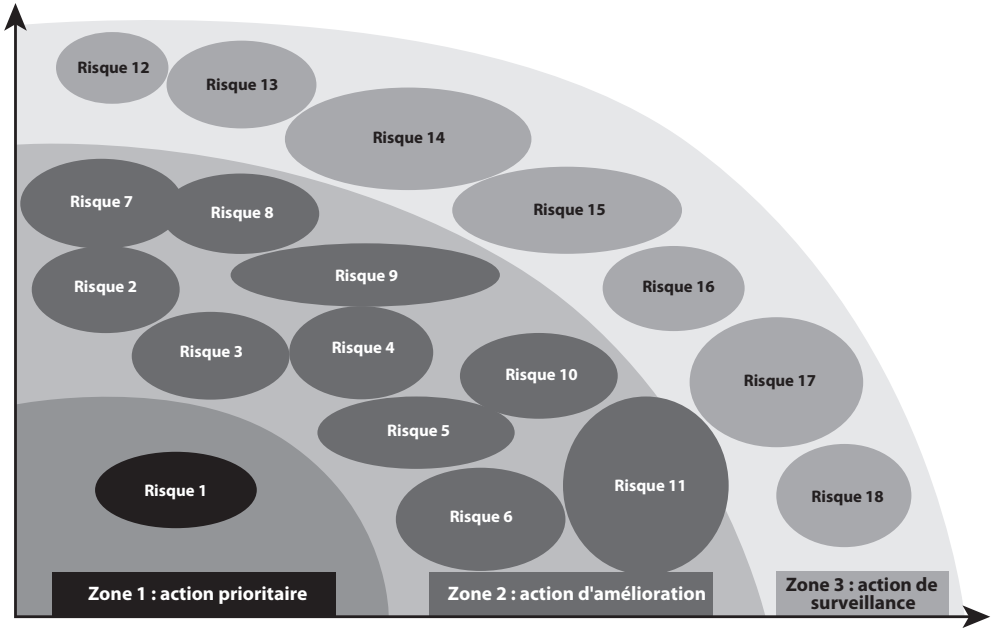
© IFACI

# ANNEXE 10

## Exemples de *reporting*

### *10.1 Carte des risques prioritaires à mettre sous contrôle*

***Synthèse des risques résiduels consolidation***








© IFACI

## 10.2 Exemple FERMA

**Table - Description des risques**

| | |
|---|---|
| 1. Nom du risque | |
| 2. Portée du risque | Description qualitative des événements, taille, type, nombre et interdépendances |
| 3. Nature du risque | En général stratégique, opérationnelle, financière, liée aux connaissances ou à la conformité |
| 4. Parties prenantes | Parties prenantes et leurs attentes |
| 5. Qualification du risque | Importance et probabilité |
| 6. Tolérance / appétence pour le risque | Perte potentielle et impact financier du risque<br>Valeur à risque<br>Probabilité et amplitude des gains / pertes potentielles<br>Objectif(s) de la maîtrise des risques et niveau désiré de performance |
| 7. Traitement du risque & mécanismes de maîtrise | Principaux moyens par quoi le risque est actuellement géré<br>Degré de confiance dans les moyens de maîtrise en place<br>Identification des protocoles pour la surveillance des risques et leur examen |
| 8. Actions d'amélioration possibles | Recommandations pour réduire le risque |
| 9. Développement de la stratégie et de la politique face au risque | Identification de la fonction responsable de développer la stratégie et la politique face à ce risque |

*Cadre de référence de la gestion des risques / FERMA (2003)*



© IFACI

## 10.3 Contrôles proportionnés à la maturité du niveau de maîtrise des risques

Cette évaluation peut par exemple s'orienter selon les critères suivants :

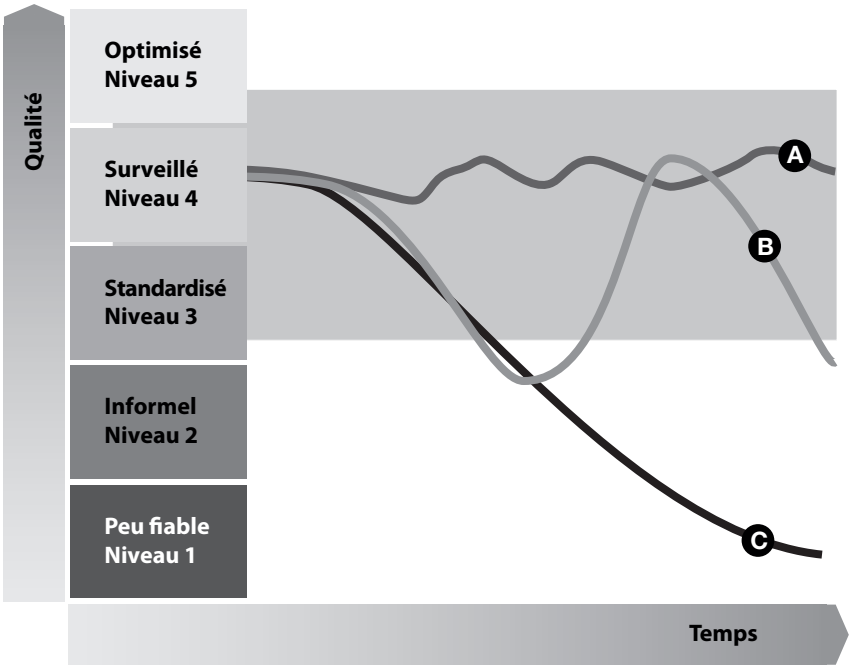
| | |
|---|---|
| **Optimisé Niveau 5** | les activités du SCI sont harmonisées avec d'autres fonctions de contrôle. La gestion des risques et le SCI sont exploités comme un système intégré. Les activités de contrôle sont largement automatisées et l'utilisation d'outils permet des ajustements rapides lorsque les conditions évoluent. |
| **Surveillé Niveau 4** | les principes d'exploitation du SCI sont décrits de manière détaillée. L'exécution des activités de contrôle est surveillée régulièrement et la traçabilité assurée. Les contrôles sont adaptés en permanence aux risques et la documentation est tenue à jour. Une fois par an, la direction reçoit un rapport sur l'évaluation du SCI (efficacité, traçabilité, efficience). Les activités de contrôle sont documentées selon un processus standardisé. Un responsable SCI coordonne et surveille les activités de contrôle. |
| **Standardisé Niveau 3** | des principes simples d'exploitation du SCI sont définis. Les processus (activités et contrôles) sont documentés. La traçabilité des contrôles effectués est assurée. Les contrôles sont régulièrement ajustés lorsque les risques évoluent. Une formation de base des collaborateurs a été organisée. |
| **Informel Niveau 2** | des contrôles internes existent mais ils ne sont pas standardisés. Les contrôles existants ne sont existants ne sont exécutés que rarement ou ne le sont pas du tout. Ils dépendent fortement des personnes ; il n'y a ni formation, ni communication les concernant. |
| **Peu fiable Niveau 1** | il n'existe pas ou pratiquement pas de contrôles internes. Selon les circonstances, les contrôles existants sont peu fiables. |

*Niveau de maturité d'un SCI (extrait de Mise en place d'un système de contrôle interne (SCI), 2e éd. / Contrôle fédéral des finances suisse. p. 14).*





© IFACI




Exigence de qualité en matière de SCI

**A** Processus avec une évaluation continue de la qualité du contrôle

**B** Contrôles ponctuels (processus d'amélioration non integré)

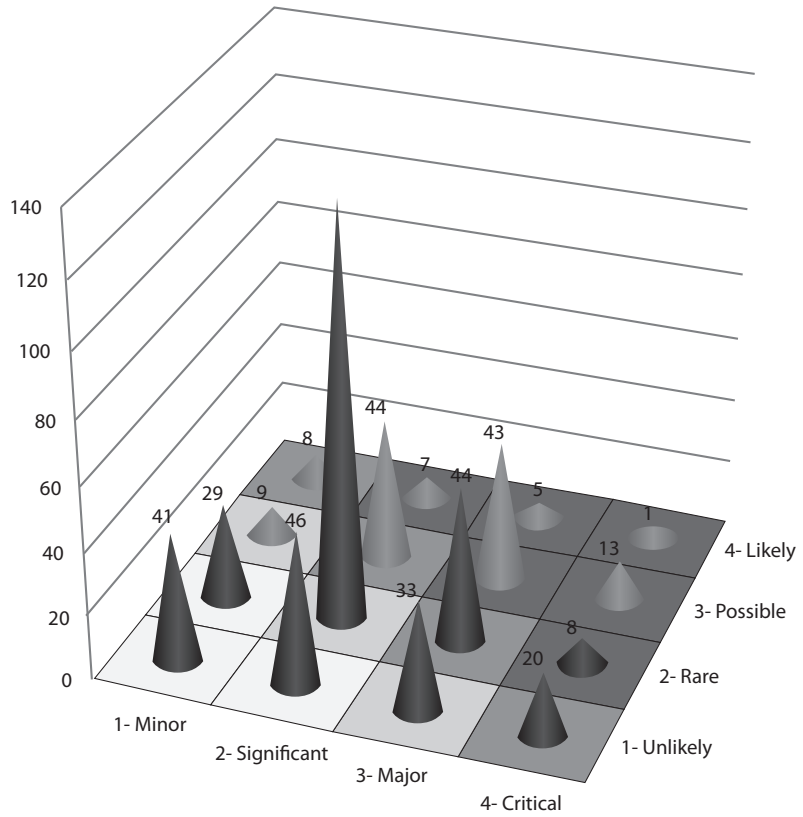
**C** Affaiblissement normal de la qualité du contrôle auf fil du temps

*Evolution d'un SCI (extrait de Mise en place d'un système de contrôle interne (SCI), 2e éd. / Contrôle fédéral des finances suisse. p. 15).*



© IFACI

## 10.4 Illustration




| | |
|---|---|
| **L = risque faible**, géré par les procédures en place | L'impact sur l'atteinte des objectifs n'est pas préoccupant, le risque est sous contrôle. |
| **M = risque modére**, un suivi spécifique doit être organisé | L'impact sur l'atteinte des objectifs est limité. Des actions doivent être entreprises mais ne sont pas urgentes. |
| **S = risque significatif**, une alerte au senior management est nécessaire | L'impact sur l'atteinte des objectifs est significatif. Nécessité de prendre des actions immédiates pour limiter le risque. |
| **H = risque élevé**, action immédiate requise | L'impact sur l'atteinte des objectifs est d'une telle ampleur que les objectifs ne seront très probablement pas atteints. Nécessité de prendre des actions immédiates pour limiter le risque, et alerter la direction. |





© IFACI

# BIBLIOGRAPHIE

## *Législation*


- Directive 2009/138/CE du Parlement européen et du conseil 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (*Solvabilité II*)
- Décret n° 2008-468 du 19 mai 2008 relatif au contrôle interne des institutions de prévoyance, des mutuelles et de leurs unions
- Décret n° 2006-287 du 13 mars 2006 relatif au contrôle interne des entreprises d'assurance et modifiant le code des assurances (partie réglementaire)
- Loi n° 2003-706 du 1er août 2003 de sécurité financière. – 2003
- Public law 107-204 [Sarbanes-Oxley Act]. – 2002
- Loi n° 2001-420 du 15 mai 2001 relative aux nouvelles régulations économiques
- Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement
- Code des assurances
- Code de la sécurité sociale
- Code de la mutualité


## *Référentiel*


- Internal Control-Integrated Framework / COSO. - 2013. [version française attendue pour début 2014]
- Trois lignes de maîtrise pour une meilleure performance : fiabiliser la stratégie par une gestion organisée des risques / AMRAE, IFACI. – [à paraître en 2013].
- IIA position paper: The Three Lines of Defense in Effective Risk Management and Control / IIA. – 2013.
- Prise de position de l'IIA : Les trois lignes de maîtrise pour une gestion des risques et une contrôle efficaces / IIA, IFACI, trad. – 2013.
- Guidance on the 8th EU company law directive: Part 2: implementing the 8th EU company law directive / ECIIA ; FERMA. – 2011.
- Guidance on the 8th EU company law directive: Article 41 / ECIIA ; FERMA. – 2010.
- Les Dispositifs de gestion des risques et de contrôle interne : Cadre de référence. / AMF. – 2010.
- Management du risque - Principes et lignes directrices : Norme internationale ISO 31000:2009 / ISO. – 2009.
- Gestion des risques - Techniques d'évaluation des risques : Norme internationale ISO 31010:2009 / ISO. – 2009.
- Le Dispositif de contrôle interne : cadre de référence : Résultats des travaux du Groupe de Place établi sous l'égide de l'AMF. – IFACI, 2007.
- Le Management des risques de l'entreprise : Cadre de référence - techniques d'application : COSO II report / IFACI ; Price Waterhouse Coopers ; Landwell& Associés. – Ed. d'organisation, 2005.
- Cadre de référence de la Gestion des Risques (2003) / AIRMIC ; ALARM ; IRM : FERMA, trad. – 2003.


© IFACI

## *Monographies*


- Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet [Cahier de la Recherche]/ Unité de Recherche Informatique de l'IFACI. – IFACI, 2013.
- Explanatory text on the proposal for guidelines on the system of governance / EIOPA. – 2013.
- Rapport annuel 2012 / ACP – 2013.
- Guide 73:2009 : Management du risque – Vocabulaire / ISO. – 2013.
- Enterprise Risk Management: Understanding and Communicating Risk Appetite. – COSO, 2012.
- Rapport annuel 2011 / ACP. – 2012.
- Gérer les risques sous solvabilité 2 / Dan Chelly ; Gildas Robert. – Argus de l'assurance, 2012.
- La Délégation de gestion en assurances de personnes : pistes pour un contrôle interne efficace [Cahier de la Recherche] / Unité de Recherche de l'IFACI. – IFACI, 2012.
- L'Efficacité des conseils d'administration : les meilleures pratiques / IIA ; traduit de l'anglais par IFACI et PWC. – Paris : IFACI, 2012.
- Board effectiveness: What works best, 2nd ed. / Catherine L. BROMILOW ; et al.. – IIA, 2011.
- L'Efficacité des comités d'audit : les meilleures pratiques / traduit de l'anglais par IFACI et PWC. – IFACI, 2011.
- Audit committee effectiveness: What works best, 4th ed.. / Catherine L. BROMILOW ; et al.. – IIA, 2011.
- Solvency II: consultation paper on the proposal for guidelines on own risk and solvency assessment [CP 008/2011]. – CEIOPS, 2011.
- Prise de position IFA - IFACI sur le rôle de l'audit interne dans le gouvernement d'entreprise : Mai 2009 / Groupe de travail IFA - IFACI. – IFACI, 2009.
- Le rôle de l'audit interne dans le gouvernement d'entreprise / IFA ; IFACI. – IFACI, 2009.
- Le rôle de l'administrateur dans la maîtrise des risques / IFA ; AMRAE. – IFA, 2009.
- CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Supervisory Reporting and Public Disclosure Requirements – (former Consultation Paper 58) / CEIOPS. – 2009.
- La gestion des risques, 2e éd. / Olivier Hassid. – Dunod, 2008.
- Mise en place d'un système de contrôle interne (SCI), 2e éd. / Contrôle fédéral des finances suisse. – 2007.
- GTAG 6 : Gérer et auditer les vulnérabilités des technologies de l'information / Sasha ROMANOSKY ; et al. . – IIA ; IFACI, 2006.
- La cartographie des risques [Cahier de la Recherche] / Groupe Professionnel « Assurance » de l'IFACI. – IFACI, 2006.


## *Périodiques*


- Les Outils informatiques au service des auditeurs et des contrôleurs internes : Leurs fonctionnalités et leurs atouts.– « Audit & Contrôle internes », n°212 décembre 2012.


Réalisation : Ebzone Communication (www.ebzone.fr)



© IFACI