IRM | institut du risk management

Rapport de projet présenté devant un Jury de Soutenance

**Expert ERM**

**Expert(e) Management des Risques Financiers et Assurantiels**

Le 15/11/2018

Par : Alexandre Guégau

Titre : Intégration de la gestion des risques opérationnels dans le déploiement d'une démarche ERM globale

Confidentialité : ☒ NON ☐ OUI (Durée : ☐ 1an ☐ 2 ans)

*Les stagiaires s'engagent à ce que les données de l'Entreprise présentées dans le cadre des travaux de la formation (rapport de projet & présentation) respectent les règles relatives à la protection des données à caractère personnel conformément aux dispositions de la Loi informatiques et Liberté n°78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004*

*Membres présents du jury :*

_____

_____

_____

_

_____

_____

***Par ma signature j'autorise la publication sur un site de diffusion de documents actuariels du rapport de projet***

*(après expiration de l'éventuel délai de confidentialité)*

Nom : Guégau

Prénom : Alexandre

Signature du stagiaire

**Si binôme :**

Nom :

Prénom :

Signature du stagiaire

# 0 SYNTHESE

L'objet du présent rapport consiste à présenter les modalités de mise en œuvre d'une démarche ERM, dans le cadre de la gestion des risques opérationnels, avec notamment une méthodologie d'évaluation, une cartographie, une gouvernance, des politiques écrites. Ce dispositif a permis d'implémenter un dispositif utile et pragmatique dans un délai relativement court.

Pour éviter toute complexité de diffusion due à la confidentialité de certaines informations, les évaluations présentées dans ce rapport ne reflètent pas la réalité des risques de la mutuelle. Le but de ce rapport n'est pas d'exposer un état des lieux de la criticité des risques opérationnels mais de présenter une démarche avec l'ensemble de ses composantes ainsi que les difficultés rencontrées et les solutions apportées.

L'exercice de cartographie des risques n'est pas une fin en soi, mais un diagnostic du niveau de risque auquel la mutuelle est confrontée. C'est donc un outil de gestion des risques qui doit être exploité et continuellement alimenté.

La mise en place d'une démarche ERM dans le cadre d'un dispositif de gestion des risques opérationnels, a pour objectif, par une meilleure maîtrise des risques, de réduire la survenance des incidents pouvant affecter notamment la qualité de service et la rentabilité de la mutuelle ainsi que le respect des engagements (Faillite de Baring en 1995, l'affaire du sentier II (Fraude fiscale) à la Société Générale en 2008, …).

Le risque opérationnel est un risque complexe à évaluer, c'est pourquoi il n'existe pas de consensus concernant la modélisation de ce risque (Paul EMBRECHTS, L'Actuariel, Juin 2015). Les différentes règlementations en vigueur aujourd'hui, notamment Solvabilité 2 où la formule standard est principalement basée sur des volumes (provisions, primes), ne permettent pas de calculer de manière précise le coût en capital lié au risque opérationnel. Un des prérequis serait d'avoir une base incidents de qualité avec une profondeur d'historique et une exhaustivité suffisantes pour réaliser des mesures de risques robustes. Les métiers n'ont pas une propension naturelle à déclarer des incidents dans la mesure où cela donne une image négative de l'activité et cela les contraint à rechercher les causes des incidents.

Ce rapport de projet se décompose en sept parties. La première partie vise à introduire la notion de gestion des risques opérationnels. La seconde partie présente la démarche ERM globale autour du dispositif de gestion des risques opérationnels. La troisième partie décrit le dispositif et les prérequis nécessaires à son déploiement. La quatrième partie présente la méthodologie utilisée pour évaluer les risques opérationnels associés aux processus. La cinquième partie détaille la phase d'entretiens, génèse des évaluations des risques. La sixième partie donne un aperçu de la cartographie des risques opérationnels créée. La septième et dernière partie, aborde l'après cartographie des risques et le rôle de cette dernière dans le pilotage des risques.
En conclusion, la démarche ERM globale associée au dispositif de gestion des risques opérationnels introduit de nouveaux objets (politiques, appétence, fonctions clés, comitologie) dans le système de gestion des risques et développe leur efficacité via les interactions entre ceux-ci.

# SOMMAIRE

# 1 DISPOSITIF DE GESTION DES RISQUES OPERATIONNELS

Un risque opérationnel est le risque de pertes liées à une défaillance ou un dysfonctionnement des processus, des systèmes d'information, des hommes ou liées à des évènements extérieurs.

Contrairement à des risques financiers, pour lesquels la mutuelle peut accepter voire augmenter son exposition selon son appétence, les risques opérationnels comme les risques de non-conformité se doivent d'être réduits au maximum. La septième partie « L'après exercice de cartographie, le pilotage des risques » détaille l'appétence de la mutuelle vis-à-vis du risque opérationnel par la mise en place de dispositifs (plan d'actions, plan de tests) spécifiques suivant la criticité résiduelle des risques.

## 1.1 Contexte Règlementaire

Les dispositions relatives au système de gestion du risque opérationnel figurent aux articles L.354-2 et R.354-2 du Code des Assurances applicables aux organismes relevant des trois codes et transposant l'article 44 de la Directive 2009/138/CE, dite "Solvabilité II". Elles sont complétées par les articles 259 et 260 du règlement délégué (UE) n°2015/35 ainsi que par le point 5 de la notice "Solvabilité II – système de gouvernance".

## 1.2 Objectifs & enjeux

Au-delà de l'aspect règlementaire, les enjeux d'un dispositif de gestion des risques opérationnels efficient consistent à :

- Améliorer sa rentabilité par la meilleure maîtrise des risques (pertes évitées) ;
- Améliorer sa réactivité en se donnant les moyens de repérer et d'anticiper les risques au lieu de les subir, de mettre ces risques sous contrôle par des actions correctrices ;
- Maîtriser ses processus et améliorer la qualité de service ;
- Développer et diffuser au sein de la mutuelle une culture de gestion des risques par l'intermédiaire d'entretiens réguliers avec les opérationnels.

Gérer ses risques opérationnels de manière efficace permet de réduire d'autres risques qui pourraient survenir, notamment le risque d'image/réputation suite à des erreurs lors de processus clés (gestion des contrats ou des investissements) et les risques règlementaires (production des reporting prudentiels dans les délais imposés par la règlementation).

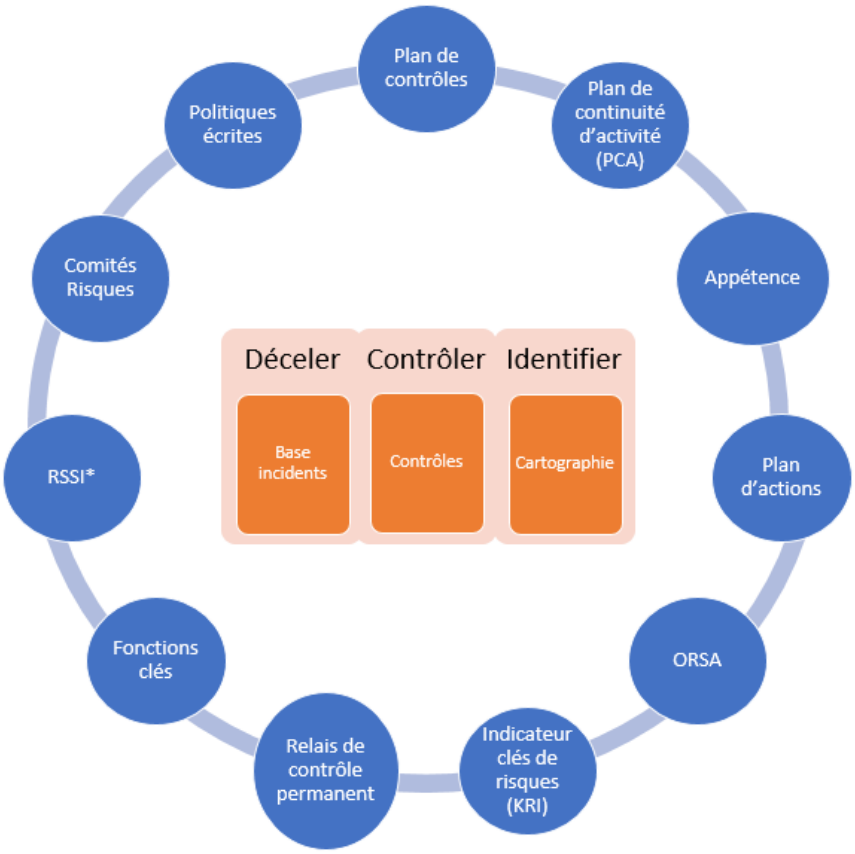
## 2 LA DEMARCHE ERM AUTOUR DU DISPOSITIF DE GESTION DES RISQUES OPERATIONNELS

L'objectif ici est d'exposer de manière visuelle la démarche ERM qui a été déployée notamment dans le cadre de la mise en place de la règlementation Solvabilité 2.

Le cœur du graphique représente la Gestion des Risques Opérationnels de base, c'est-à-dire sans démarche ERM globale. Elle était habituellement traitée de manière indépendante et cantonnée à une base incidents, des contrôles et une cartographie des risques. Les éléments satellites représentent la démarche ERM globale déployée notamment en réponse à la règlementation Solvabilité 2 qui intègrent les bonnes pratiques actuelles en matière de gestion des risques. Ceci permettant d'apprécier la Gestion des Risques Opérationnels de manière plus globale et ainsi de diffuser d'avantage la culture du risque. L'ensemble de ces éléments satellites est détaillé dans les différentes parties de ce projet de rapport.

Certains éléments d'ores et déjà existants avant la mise en place de Solvabilité 2 tels que le RSSI (*Responsable de la Sécurité des Systèmes d'Information) et le plan de continuité d'activité (PCA) se retrouvent désormais en interaction avec les autres objets du dispositif de gestion des risques opérationnels.

Pour sensibiliser le Conseil d'Administration de la mutuelle sur la nécessité d'un PCA efficace et le promouvoir en interne, des scénarios de stress sur des risques opérationnels tels que la crue, les incendies et les cyber risques ont été introduits dans le processus ORSA/EIRS (*Own Risk and Solvency Assesment* – Evaluation Interne des Risques et de la Solvabilité).



# 3 PRESENTATION DU DISPOSITIF & PREREQUIS

Cette partie présente la démarche préalable à l'identification des risques, en particulier le calibrage des référentiels nécessaires à l'élaboration de la cartographie.

## 3.1 Démarche *Bottom-Up*

Afin d'évaluer les risques opérationnels et conformément à la politique écrite de gestion des risques opérationnels mise à jour, il a été convenu d'adopter une démarche dite *Bottom-Up* (ascendante) qui consiste à faire identifier les risques par les opérationnels, c'est-à-dire ceux chargés d'exécuter quotidiennement les activités. Pour ce faire, cette démarche s'appuie notamment sur un référentiel de processus propre à la mutuelle et un référentiel de risques opérationnels génériques.

La démarche *Bottom-Up* adoptée par la mutuelle consiste, à l'occasion de la description des processus, à faire identifier et évaluer les risques opérationnels par les responsables des processus. Ces travaux sont réalisés annuellement lors d'entretiens menés par la fonction Gestion des Risques.

La fonction Gestion des Risques n'a pas toutes les compétences pour objectiver les éléments communiqués par les opérationnels lors de ces entretiens, elle fait donc appel, quand cela est nécessaire, à des experts dans leur domaine, notamment au responsable de la fonction clé Vérification de la Conformité et au Responsable de la Sécurité des Systèmes d'Information (RSSI).

En particulier, les risques opérationnels ayant un aspect règlementaire, par exemple le processus LCB-FT (Lutte Contre le Blanchiment et le Financement du Terrorisme), sont évalués par le responsable de la fonction clé Vérification de la Conformité, lors de l'entretien ou dans le cadre d'entretiens spécifiques. Le responsable de la fonction clé Vérification de la Conformité établit une cartographie des risques de non-conformité qui est ensuite agrégée dans la cartographie des risques opérationnels.

La mise à jour de la cartographie des risques opérationnels sera effectuée chaque année au cours du dernier trimestre, ceci permettant d'avoir au 1er trimestre de l'année suivante une cartographie à jour nécessaire pour la définition des scénarios ORSA. De plus, la revue des évaluations avec les responsables de processus avant la fin de l'année permet de déterminer si des moyens supplémentaires (élaboration budgétaire) sont à prévoir pour la mise en œuvre des plans d'actions. Les actions correctrices à mener peuvent ainsi débuter dès le début de l'année suivante.

## 3.2 Mise en place de référentiels

### 3.2.1 Référentiel de processus

Afin de structurer la démarche globale de gestion des risques et faciliter les travaux de reporting et de synthèse, un référentiel de processus a été défini pour l'ensemble des activités de la mutuelle. Ce référentiel modélise les activités de la mutuelle en 3 familles homogènes de processus (Métier, Support et Stratégique) et avec 3 niveaux de classement. Voici un exemple de processus « Processus de niveau 3 » pour chacune des familles citées :

| Famille | Processus niveau 1 | Processus niveau 2 | Processus niveau 3 |
|---|---|---|---|
| Stratégique | Développement stratégique | Définition de la stratégie commerciale | Business plan |
| Métier | Gestion des garanties | Prestations | Gestion des rachats et transferts en sortie |
| Support | Gestion des moyens généraux | Traitement du courrier entrant/sortant | Traitement du courrier entrant/sortant |

Ce référentiel permet de vérifier que l'ensemble des activités de la mutuelle sont prises en compte et facilite la résolution des incidents puisque chaque processus est associé à un responsable. Ce référentiel est susceptible d'évoluer en fonction des travaux de description des processus et de cartographie. Ce référentiel permet de déterminer les activités (processus) à cartographier. Un extrait du référentiel est présenté en Annexe 1 « Extrait du référentiel de processus ».

### 3.2.2 Référentiel de risques

Le référentiel des risques recense l'ensemble des événements potentiels ayant un impact opérationnel sur les activités.

Le référentiel des risques opérationnels, défini en interne, est organisé sur trois niveaux :

- Le premier, directement issu de la réglementation Bâle II, est fixe. Il assure un reporting en phase avec les meilleures pratiques des secteurs Banque et Assurances.
- Les deux autres niveaux (classes de niveau 2 et 3) du référentiel sont propres à l'activité de la mutuelle. Basés sur le référentiel IFACI (Institut Français de l'Audit et du Contrôle Internes) et sur des réflexions internes, ils permettent un reporting plus fonctionnel et mieux adapté aux spécificités de la mutuelle.

Un extrait du référentiel est présenté en Annexe 2 « Extrait du référentiel de risques ».

### 3.2.3 Référentiel des causes

Ce référentiel recense les causes, internes comme externes, qui permettent la survenance du risque. Ce référentiel est présenté dans l'Annexe 3 « Référentiel de causes ».

### 3.2.4 Synthèse des référentiels

| Référentiel des processus | Référentiel des risques | Référentiel des causes |
|---|---|---|
| • Il permet de déterminer les activités à cartographier | • Il recense l'ensemble des risques opérationnels de toutes les activités de la Mutuelle | • Il recense les causes, internes comme externes, qui permettent la survenance du risque |

## 3.3 Croisement référentiels risques / Processus

Le croisement entre les référentiels de risques et des processus permet d'affecter à chaque processus les risques associés. Comme indiqué ci-dessous, le croisement s'effectue au niveau 3 des 2 référentiels.


Les risques de niveau 3 à évaluer pour un processus donné sont détaillés à titre d'exemple dans la partie « 6.2 Focus sur un processus précis ». La méthodologie d'évaluation des risques, et par conséquent l'évaluation de la criticité du processus auxquels sont rattachés ces risques, est détaillée dans la partie suivante. En se basant sur ces différents éléments, le cadre de la démarche de cartographie est défini et les travaux d'évaluations peuvent débuter.

# 4 METHODOLOGIE D'EVALUATION

L'objectif de cette partie est d'évaluer le risque brut, c'est-à-dire de quantifier les impacts et la fréquence du risque en faisant abstraction de tous les éléments de maîtrise du risque (EMR) en place, ainsi que le risque net qui est l'évaluation du risque en prenant en compte tous les éléments de maitrise (EMR) en place.

La base incidents, élément clé de la démarche ERM, ayant été déployée en même temps que l'élaboration de la méthodologie d'évaluation des risques opérationnels, elle n'a pas pu contribuer pleinement à l'évaluation des risques. Cependant, un incident étant un risque avéré, la base incidents permettra, lors du prochain exercice de cartographie, de prendre en compte les incidents survenus.

## 4.1 Evaluation du risque brut

Le risque brut, est le risque propre à l'exercice du processus sans prise en compte des moyens de maîtrise en place.

L'évaluation de la criticité du risque brut se compose de :

- L'évaluation de sa probabilité de survenance ;
- L'évaluation de ses impacts (financier, règlementaire, image/réputation).

Ces éléments sont présentés, en détails, en annexe 4 « Méthodologie d'évaluation du risque brut ».

La criticité du risque brut se détermine en croisant l'impact et la fréquence par l'intermédiaire de la matrice suivante :

**CRITICITE DU RISQUE BRUT**

| Impact potentiel | Faible | Moyenne | Forte | Très forte |
|---|---|---|---|---|
| Critique | Majeur | Majeur | Majeur | Majeur |
| Fort | Elevé | Elevé | Elevé | Majeur |
| Modéré | Modéré | Modéré | Elevé | Elevé |
| Faible | Mineur | Modéré | Modéré | Elevé |

Probabilité de survenance

Pour une plus grande adhésion et pour qu'elles soient adaptées à la taille de la mutuelle, les échelles (impact et survenance) ont été calibrées en collaboration avec l'ensemble des fonctions clés et présentées en Comité Opérationnel de Gestion des Risques avant de débuter la phase d'évaluation des risques. L'échelle des impacts a été calibrée en prenant en compte d'une part une perte sur le résultat de l'année et d'autre part le nombre d'adhérents impacté par la survenance du risque. Dans la mutualité, les administrateurs étant adhérents eux-mêmes et représentants de l'ensemble des adhérents, leur propension à veiller sur l'intérêt général est renforcée par nature. La pondération de

l'axe risque de réputation dans l'évaluation du risque net est ainsi supérieure à la moyenne du marché de l'Assurance.

Plus concrètement, lors de l'élaboration de la méthodologie, il avait été retenu d'effectuer la moyenne entre les différentes natures d'impacts (financier, réglementaire, image/réputation). A la suite des premiers entretiens, la méthodologie a été revue pour être plus prudente et prendre en compte la particularité de la mutualité mentionnée précédemment : l'impact est évalué comme l'impact maximal entre les 3 natures d'impacts.

La première méthodologie entrainait une sous-évaluation de l'impact car les 3 types étaient équipondérés. Par exemple, un risque ayant un impact financier faible, un impact en termes d'image et de réputation faible mais un impact réglementaire critique, car pouvant entrainer la responsabilité pénale des dirigeants effectifs, aurait eu un impact modéré alors qu'avec la méthodologie du maximum, l'impact est critique et reflète ainsi mieux l'impact que pourrait avoir la réalisation de ce risque.

## 4.2 Evaluation du dispositif de maîtrise des risques

### 4.2.1 Méthodologie

Le Dispositif de Maîtrise des Risques (DMR) est l'ensemble des moyens de maîtrise mis en place pour limiter les risques : contrôles opérationnels, séparation des tâches (saisie/validation)... Ils sont répertoriés dans des catégories spécifiques qui en facilitent l'analyse et l'évaluation. Ces catégories sont appelées familles de moyens de maîtrise et présentées en Annexe 5 « Famille de moyens de maitrise ».

Il est nécessaire de recenser les éléments de maîtrise pour chacune des familles de moyens de maîtrise identifiées. L'évaluation est fonction d'un critère de formalisation et d'un critère d'efficacité à couvrir le risque (cf. Annexe 6 « Critères d'évaluation des moyens de maitrise »).

Par principe de prudence, la cotation du DMR considérée est égale à la moyenne des scores des éléments de maîtrise du risque (EMR) qui le composent. Utiliser le maximum aurait surévalué l'efficacité des EMR. Une évaluation globale du DMR est in fine réalisée.

### 4.2.2 Objectiver les informations communiquées par le responsable de processus sur les EMR existants et ceux à créer

Comme indiqué dans la partie précédente, le DMR du risque concerné est le résultat de la moyenne de ses EMR. Il peut exister un biais lors de l'utilisation de cette méthode, si par exemple sur un risque où il n'existe qu'un seul EMR et que celui-ci est qualifié de « Très significatif ». L'évaluation du risque net sera fortement réduite par cet EMR « Très Significatif ». Il est donc très important que la personne qui mène l'entretien prenne connaissance du processus en amont de l'entretien et qu'il soit force de proposition auprès du responsable de processus pour lui faire intégrer, avant même de discuter des plans d'actions, des propositions de nouveaux EMR qui seront qualifiés en « Inexistant ». Cette phase va permettre, dès l'évaluation du DMR, d'évoquer des pistes d'améliorations concernant la maîtrise de ce risque et de manière plus globale du processus.

Il est important durant l'entretien avec le responsable de processus de prendre le temps de se détacher de l'aspect opérationnel pour analyser les différents éléments composants le DMR. Aborder l'entretien comme une collaboration et non un contrôle de l'existant, permet de gagner du temps et de recueillir plus d'éléments sur les contrôles en place et les difficultés inhérentes au processus (exemple : contrôle visuel car impossibilité d'extraire la base).

### 4.2.3 La problématique du poids des différents EMR dans l'évaluation du DMR

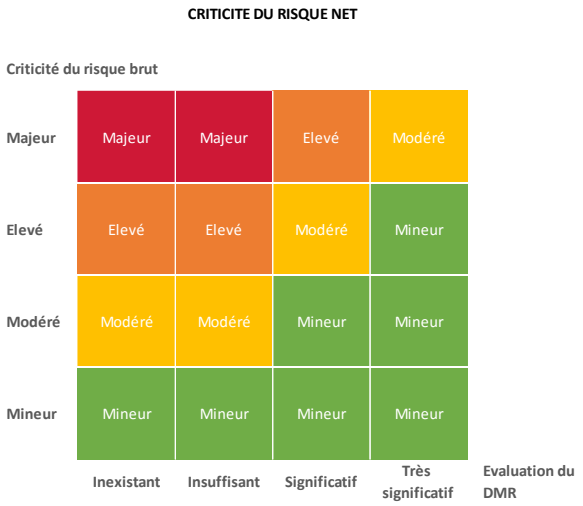
Le poids des EMR (Eléments de Maitrise du Risque) est équiprobable dans l'évaluation du DMR d'un risque, c'est pourquoi dans certains cas l'évaluation globale du DMR peut être forcée pour refléter au mieux la réalité. Dans le questionnaire, une ligne en dessous de celle calculant automatiquement l'évaluation globale du DMR a été rajoutée : c'est l'évaluation forcée du DMR.
Pour illustrer ce besoin, il faut prendre l'exemple d'un risque qui a un DMR composé des 3 EMR suivants :

- EMR N°1 : Moyens Humains
  - Gestionnaires experts formés chaque année (Documenté, traçable et efficace)
  - EMR qualifié de « Significatif »
- EMR N°2 : Contrôles humains
  - Contrôles « visuels » (Non documenté, non traçable et efficace)
  - EMR qualifié de « Insuffisant »
- EMR N°3 : Plan de continuité
  - Serveurs doublés (Documenté, traçable et Très efficace)
  - EMR qualifié de « Très Significatif »

L'évaluation du DMR va être calculée automatiquement en « Significatif » alors que la partie contrôle n'est ni documentée ni traçable donc aucun moyen de vérifier, a posteriori, les contrôles effectués et les anomalies détectées. L'évaluation forcée du DMR va permettre d'atténuer le calcul automatique et ainsi l'évaluer à « Insuffisant », par conséquent un plan d'actions/de remédiation sera indiqué pour l'EMR N°2.

## 4.3 Déduction du risque net

Le risque net, est le risque qui subsiste, malgré la mise en place de moyens de maîtrise. C'est le point d'intersection entre la gravité du risque et son niveau de maîtrise actuel.




La cartographie du risque net est un élément de caractérisation de l'appétence associée au risque opérationnel, ceci est détaillé dans la septième partie « L'après exercice de cartographie, le pilotage des risques ».

### 4.4 Evaluation de la criticité du processus

Pour un même processus, il a été calculé la criticité nette de chaque risque associé à ce processus. Pour obtenir une vision consolidée, on regroupe les risques nets par processus, par l'intermédiaire d'un premier filtre sur les processus ayant un ou plusieurs risques nets qualifiés de « Majeur ». Dans la septième partie « L'après exercice de cartographie, le pilotage des risques », on détaille l'utilisation de la cartographie dans un cadre de contrôle, de réduction des risques et d'amélioration des processus.

# 5 CAMPAGNE D'ENTRETIENS

## 5.1 Objectif de l'entretien

L'objectif de l'entretien est d'évaluer, pour un processus, les risques bruts et les dispositifs de maîtrise des risques pour en déduire les risques nets. Il se déroule avec le responsable du processus, à savoir un responsable opérationnel qui, selon l'organigramme et le processus concerné, peut-être un responsable de pôle/service/département, un membre du Comité de Direction ou, exceptionnellement, un opérationnel.

## 5.2 Planification, préparation et déroulement des entretiens

L'identification et l'évaluation des risques opérationnels étant un exercice complexe et encore peu habituel au sein de la mutuelle, la planification de chaque entretien s'accompagne de la transmission des éléments suivants 2 semaines en amont : le support pédagogique rappelant la démarche, les différents référentiels et le questionnaire. Cela laisse le temps au responsable de processus interviewé de mettre à jour la liste des risques préremplie par la fonction Gestion des Risques et de la compléter de la liste des éléments de maîtrise en place. Le questionnaire est un fichier comprenant 3 onglets correspondant à la carte d'identité du processus, à la fiche des risques et aux moyens de maîtrise. Ces onglets sont détaillés dans la partie suivante où un focus est réalisé sur un processus donné.

Le but de l'entretien est d'identifier et évaluer les risques opérationnels auxquels le processus est exposé, ainsi que les moyens de maîtrise en place et ceux à mettre en place. Les différentes phases de l'entretien sont décrites en Annexe 7 « Phases de l'entretien ». Tout au long de l'entretien, il est important de sensibiliser au bénéfice des EMR. Les entretiens permettent aussi de remonter des incidents survenus dans le passé et souvent méconnus. Au total plus de 55 entretiens de 3 heures ont été réalisés sur une période de 3 mois.

## 5.3 Difficultés rencontrées lors des entretiens

Au fil des entretiens, les problématiques suivantes remontaient de manière assez régulière :

- La difficulté à évaluer le risque et ainsi faire abstraction de l'ensemble des éléments de maîtrise en place,
- La vision parfois optimiste des responsables de processus sur le niveau de risque brut et de l'efficacité des DMR (procédures, contrôles, …).

## 5.4 Restitutions des entretiens

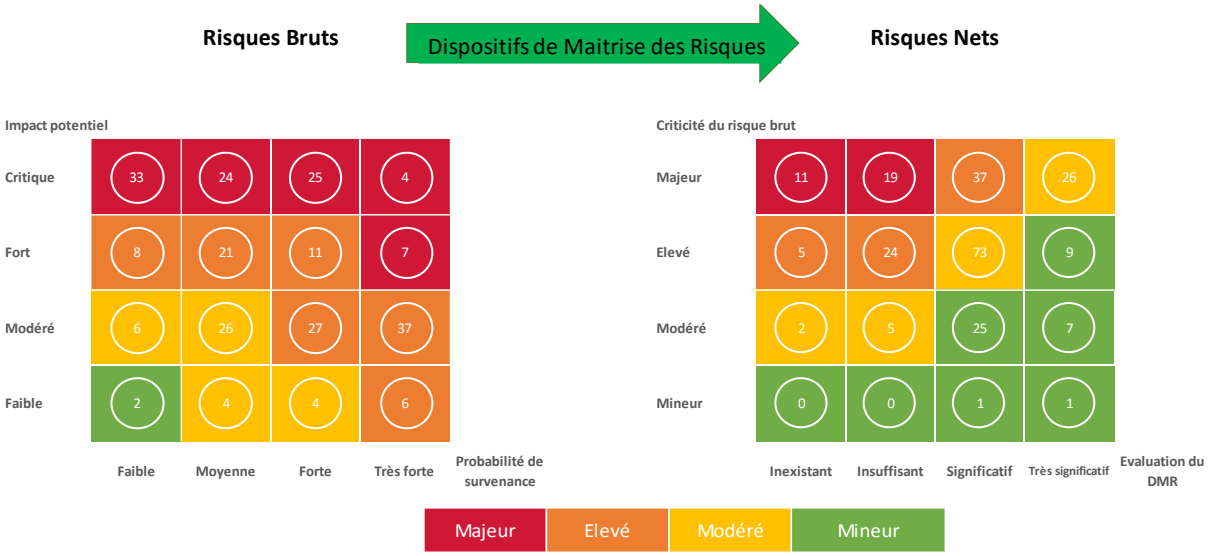
À la suite de l'entretien, la fonction Gestion des Risques consolide l'ensemble des informations échangées notamment les éventuels plans d'actions à mettre en œuvre et envoie cette restitution au responsable du processus pour validation.

En cas de désaccord entre la fonction Gestion des Risques et les responsables de processus, un processus d'escalade est prévu notamment auprès du Dirigeant Opérationnel voire des administrateurs (Comité des Risques) dans des cas plus critiques. Ces éléments sont intégrés dans la politique de gestion des risques opérationnels, validée annuellement par le Conseil d'Administration.
Dès la validation de la restitution effectuée, le processus est intégré dans la cartographie des risques opérationnels. Les plans d'actions ont vocation à être suivis et présentés lors des comités des risques.

# 6 CARTOGRAPHIE DES RISQUES

## 6.1 Représentation / visuel

Pour replacer l'exercice de cartographie dans son contexte, 55 processus de niveau 3 ont été évalués et 245 risques opérationnels (couple « processus-risque ») ont été identifiés.




*Dans un souci de confidentialité, les données ont été volontairement modifiées et les intitulés des processus ont été retirés.*

## 6.2 Focus sur un processus précis

**Dans un souci de confidentialité, l'ensemble des informations présentes dans cette partie sont fictives et ont été produites à titre d'exemple pour illustrer la démarche.** L'évaluation des risques sur un processus précis est décrite en Annexe 8 « Focus sur un processus précis ».

# 7 L'APRES EXERCICE DE CARTOGRAPHIE, LE PILOTAGE DES RISQUES

A ce stade, la cartographie des risques opérationnels permet d'obtenir une vision consolidée et quantifiée des risques se référant à l'ensemble des processus opérationnels. L'exercice de cartographie des risques n'est pas une fin en soi, mais un diagnostic du niveau de risques auquel la mutuelle est confrontée. C'est donc un outil de gestion des risques qui doit être exploité. Cette partie expose les tâches à mener pour réduire les risques, faire vivre cette cartographie dans le temps et l'intégrer dans une démarche plus globale de gestion des risques.

La politique de gestion des risques opérationnels reprend les grandes lignes de la méthodologie exposées dans les parties précédentes ainsi que la plupart des différents notions et dispositifs présentés dans les parties suivantes. Cette politique est la formalisation de la démarche ERM qui gravite autour

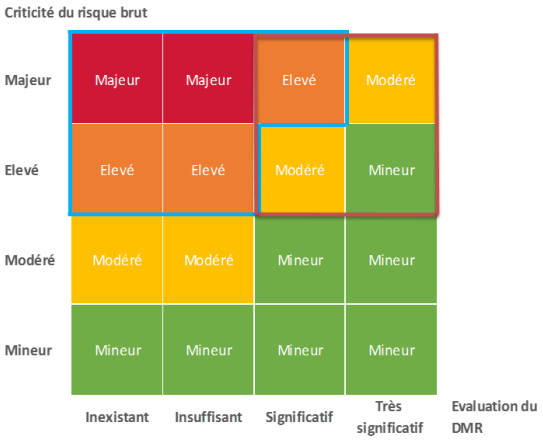
de la gestion du risque opérationnel (démarche, méthodologie, responsabilité, reporting, plan de contrôle, plan d'actions, communication et diffusion de la culture du risque).

**La démarche ERM permet aussi d'optimiser la situation au travers de la méthodologie et de l'organisation. Lors de l'évaluation des risques opérationnels, la Gestion des Risques va demander, sur un processus donné, les livrables attendus, le calendrier, la charge, le processus de validation des éléments clés. Ainsi remettre à plat ces éléments va permettre, avec une vision plus globale, d'optimiser certaines tâches notamment via des actions correctrices et donc de réduire les délais de production.**

## 7.1 Définition des plans d'actions et du plan de tests

Les plans d'actions à mettre en place cibleront les processus ayant un risque brut « Majeur » et des DMR « Insuffisant » ou « Inexistant ». Seront priorisés les processus ayant le plus grand nombre de risques nets « Majeur ». Le cadre bleu, de la matrice suivante, cible les risques des processus concernés par la mise en place de plans d'actions. Les plans d'actions définissent les actions complémentaires aux moyens de maîtrise à mettre en œuvre pour couvrir les risques opérationnels auxquels est exposée la mutuelle.

**Niveau de criticité du risque net**




Les plans d'actions contribuent à la maîtrise des activités en évitant qu'un incident opérationnel ne se reproduise, qu'un nouveau risque émerge ou que les impacts d'un risque ne soient trop importants. Le Contrôle Interne effectue des points réguliers avec le responsable du processus pour s'assurer de la mise en œuvre des actions correctrices. Le Contrôle Interne présente en Comité Opérationnel de Gestion des Risques une vision consolidée de l'avancement des plans d'actions. En cas de difficultés dans la mise en œuvre d'un plan d'actions, ces points seront remontés par la fonction Gestion des Risques au Dirigeant Opérationnel qui pourra arbitrer et/ou reprioriser les actions correctrices.

Le plan de tests du Contrôle Interne va avoir pour but d'aller vérifier l'efficacité des DMR les plus efficaces pour des processus ayant des risques bruts qualifiés de « Majeur ». Le cadre rouge, sur la matrice, cible les risques des processus concernés par le plan de tests/contrôles qui sera effectué par le Contrôle Internet et/ou le responsable de fonction clé Vérification de la Conformité. Le plan de tests du Contrôle Interne pour un semestre, peut être, d'aller effectuer des tests sur les 5 processus combinant un nombre important de risques majeurs et des DMR, au minimum, qualifiés de « Significatif ». Lors de

la définition des plans de tests, il est important de se coordonner avec l'ensemble des fonctions clés et notamment l'Audit Interne pour ne pas solliciter deux fois les mêmes personnes.

**Délimiter dans la cartographie les risques nets nécessitant un plan d'actions immédiat, ceux nécessitant un plan de tests, et les autres pour lesquels la mobilisation des ressources de la mutuelle en fonction de la criticité des risques n'est pas optimale donc aucune action n'est requise, caractérise l'appétence aux risques liée aux risques opérationnels. La cartographie des risques nets est ainsi un outil permettant de prioriser les actions à mener.**

## 7.2 Eléments modifiant l'évaluation d'un risque – interactions avec les Fonctions clés

La cartographie étant un outil dynamique dans le temps, elle peut être modifiée par les évènements ou éléments suivants :

- Incidents remontés via la base incidents (Contrôle Interne)
- Nouvelle campagne d'entretiens avec prise en compte des plans d'actions définis lors de la précédente campagne (Gestion des Risques)
- Résultats des plans de tests (Contrôle Interne et Vérification de la Conformité)
- Constats présents dans le rapport actuariel notamment les problématiques afférentes à la qualité des données (Fonction Actuarielle)
- Résultats d'audit (Audit Interne)

La cartographie des risques opérationnels sert aussi à orienter le plan d'Audit Interne.

Les différentes interactions sont décrites en Annexe 9 « Interaction autour de la cartographie des risques opérationnels ».

## 7.3 Lien avec le Plan de Continuité d'Activité

Une vision des processus opérationnels plus claire par l'intermédiaire des différents référentiels présentés et de la cartographie ainsi que la mise en place de plans d'actions vont permettre d'améliorer le Plan de Continuité d'Activité (PCA) en se basant sur les travaux de cartographie des risques opérationnels.

Par exemple, acter un plan d'actions indiquant la mise en place d'un entrepôt de données pour dématérialiser les actes de gestion afin d'automatiser les contrôles, améliorer la piste d'audit et réduire les manipulations (diminue la survenance des incidents) va aussi permettre lors d'une indisponibilité des locaux de pouvoir accéder à ces documents à distance.

La rédaction d'une politique de PCA a permis de renforcer le dispositif au travers notamment de la définition d'une appétence sous la forme notamment d'un délai maximum d'interruption de l'activité (DMIA).

## 7.4 Organiser le dispositif et systématiser les contrôles pour réduire les risques

En plus du Contrôle Interne et des fonctions clés, déployer des relais de contrôle permanent dans les différents départements et directions permet de systématiser les contrôles et la remontée des incidents. Le Contrôle Interne accompagne et alimente ces relais notamment sur les contrôles à effectuer et les reporting à produire.

## 7.5 Communication, formation diffusion de la culture des risques

Pour diffuser la culture des risques, il est important de communiquer de manière récurrente sur la situation en termes de risques notamment lors des différents comités. De manière trimestrielle, la fonction Gestion des Risques et le Contrôle Interne communiquent aux comités en lien avec la gestion des risques les informations suivantes :

- Les risques majeurs
- Les Incidents majeurs
- Le suivi des plans d'actions
- Le bilan des plans de tests
- Les rapports d'activité des relais de contrôle permanent
- L'avancement du Plan de Continuité d'Activité

L'étape suivante sera, au lieu de restituer la cartographie des risques aux différents comités des risques de manière globale, de mettre en place des réunions de travail par direction ou par service pour aller plus loin dans l'analyse, instaurer un dialogue constructif et conseiller les opérationnels au niveau des contrôles à mettre en place.

Dans une démarche ERM plus globale, la mise en place d'indicateurs de risque clés (KRI – *Key Risk Indicator*) comme l'évolution des réclamations clients ou des renonciations peuvent permettre d'anticiper et prévenir la dérive d'indicateurs de performance des processus clés (KPI – *Key Performance Indicator*) comme le nombre de nouveaux adhérents ou de nouveaux contrats.
Dans un dispositif de contrôles plus mature, des indicateurs de contrôles clés (KCI - *Key Control Indicator*) peuvent être utilisés pour suivre l'efficacité des contrôles comme la fréquence de mise à jour des anti-virus sur les serveurs ou le temps moyen de traitement d'un incident.

La diffusion de la culture des risques passe aussi par le rapport ORSA où la cartographie des risques opérationnels est utilisée comme base de réflexion pour la définition des scénarios de risques opérationnels.
De manière plus ponctuelle, la culture des risques peut être diffusée au sein de la mutuelle par le biais de communications ou de présentations adaptées par thématique en fonction de l'actualité :

- Crue et inondations si les évènements de juin 2016 se reproduisent à Paris,
- Neige si les évènements de février 2018 se reproduisent à Paris,
- Pandémie à l'approche de l'hiver.

Plus globalement, une présentation de la fonction et du système de gestion des risques ainsi que du dispositif de contrôle interne est effectuée aux nouveaux salariés de la mutuelle.

# 8 CONCLUSION

Les différents éléments présentés dans ce mémoire ont permis de mettre en place, sur une période restreinte, une base incidents, une première cartographie des risques opérationnels fondée sur des entretiens avec les opérationnels et de la faire interagir avec l'ensemble des composantes satellites de la démarche ERM globale présentée.

La double casquette Gestion des Risques et Contrôle Interne ainsi que le rattachement direct au Dirigeant Opérationnel a permis de mettre en place un dispositif de gestion des risques opérationnel plus rapidement et de l'intégrer dans une revue globale du système de gestion des risques.

La cartographie n'est qu'une étape dans la démarche de gestion des risques opérationnels. Les plans d'actions et de contrôles à mettre en place ou à effectuer permettent de donner de la valeur ajoutée à cette démarche par des actes concrets, notamment la réduction des risques et plus globalement participer à la reprise d'activité en cas d'évènements majeurs, et d'améliorer la rentabilité et la qualité de services de la mutuelle.

L'application d'une démarche ERM dans le cadre du risque opérationnel permet d'accroître l'efficacité du dispositif via les politiques écrites qui précisent la gouvernance et les interactions entre les différentes parties prenantes, les comités des risques (Comité Opérationnel de Gestion des Risques et Comité des Risques), l'appétence au risque avec les risques qui doivent faire l'objet de plans d'actions et remontés auprès du Dirigeant Opérationnel (Cadre bleu - Partie 7.1) et les risques qui doivent être intégrés dans les plans de tests (Cadre rouge - Partie 7.1), la cartographie, la base incidents, les rapports de contrôles, le suivi des plans d'actions, les reporting trimestriels intégrant les incidents et les risques majeurs sur la période, l'ORSA, la diffusion de la culture du risque.

Pour une meilleure compréhension du dispositif de contrôle interne, qui est étroitement lié au dispositif de gestion des risques opérationnels, il est important que chaque collaborateur connaisse sa place dans le dispositif de contrôle interne ainsi que sa contribution à ce dernier.

# 9 BIBLIOGRAPHIE


- « La Gestion des Risques en Assurance » : Axelle Brault-Fonters, Nicolas Guillaume et Fabien Raviard - L'argus De L'assurance - Les Fondamentaux De L'assurance - 1 Juin 2016

- « Entretien avec Paul Embrechts », l'actuarielle, Florence Puybareau – 29 mai 2015

# 10 ANNEXES

## Annexe 1 : Extrait du référentiel de processus

| Famille | Processus niveau 1 | Processus niveau 2 | Processus niveau 3 |
|---|---|---|---|
| Métier | Gestion des garanties | Adhésions et renonciations | **Gestion des adhésions** |
| | | | **Gestion des renonciations et des "sans effet"** |
| | | Vie de la garantie | **Modification de la garantie** |
| | | | **Gestion manuelle des avances** |
| | | | **Envoi des relevés obligatoires à l'adhérent** |
| | | | **Dépôts réglementaires et déclarations fiscales** |
| | | | **Gestion des contrats en déshérence** |
| | | Prestations | **Gestion des rachats et transferts en sortie** |
| | | | **Gestion des rentes** |
| | | | **Gestion des décès** |
| | | Relation adhérents | **Traitement des réclamations** |

## Annexe 2 : Extrait du référentiel de risques

| Ref N1 | FAMILLE DE RISQUES OPERATIONNELS | Ref N2 | RISQUES OPERATIONNELS NIVEAU 2 | Ref N3 | RISQUES OPERATIONNELS NIVEAU 3 | EXEMPLES DE RISQUES |
|---|---|---|---|---|---|---|
| O5 | DOMMAGES AUX ACTIFS CORPORELS | O5.1 | Catastrophes et événements majeurs d'origine naturelle | O5.1.1 | Catastrophes et autres sinistres exogènes à la mutuelle | Risque d'inondation, tempête, tremblement de terre, Pandémie |
| O5 | DOMMAGES AUX ACTIFS CORPORELS | O5.2 | Catastrophes et événements majeurs d'origine humaine | O5.2.1 | Catastrophes et événements majeurs d'origine humaine | Risques incendie, dégâts des eaux affectant la disponibilité des locaux de la mutuelle<br>Risques sociaux-politiques y compris le terrorisme, le vandalisme |

## Annexe 3 : Référentiel de causes

| Cause | Description | Exemples |
|---|---|---|
| Environnement externe | Actions par des agents externes à la mutuelle | - Attaques criminelles ou terroristes (y.c. phishing, déni de service, diverses formes de fraude par des individus ou des groupes,...) |
| | | - Catastrophes naturelles (inondations, vent, feu sauvage, tempête, tremblement de terre,...) |
| | | - Troubles causés par l'homme (grève, indisponibilité des transports publics,...) |
| | | - Environnement politique, social et culturel (évolutions réglementaires, conflit civil, émeute,...) |
| | | - Personnel chez les sous-traitants et les fournisseurs |
| Humain | Facteurs liés aux actions du personnel ou de la direction de la mutuelle | - Ressources inadéquates (compétences, nombre d'ETP, personnes clés,...) |
| | | - Activités criminelles par du personnel interne / externe (vol, fraude, dommage causé aux systèmes,...) |
| | | - Management et contrôle des équipes (communication insuffisante / incorrecte, supervision insuffisante,...) |
| | | - Erreur humaine (mauvaise compréhension / interprétation / décision / action non délibérée) |
| | | - Activité non autorisée (mauvaise compréhension / interprétation / décision / action délibérée) |
| Processus | Facteurs liés à l'organisation de la mutuelle et à certains grands processus de gestion | - Structure organisationnelle |
| | | - Conception du process (complexité, transparence, documentation,...) |
| | | - Politique / Procédure inadéquate (non respectée, manquante / non accessible, incompréhensible, incomplète, obsolète,...) |
| | | - Séparation des tâches inadéquate |
| | | - Qualité des données (incomplète, incorrecte, format erroné, tardive,...) |
| Systèmes | Facteurs liés aux insuffisances ou aux défaillances de la technologie interne, des systèmes physiques et de communication | - Matériel - Maintenance inadéquate (PC, imprimantes, claviers, diagnostics / états des lieux périodiques non effectués,...) |
| | | - Matériel - Dégradation de la performance (fonctionnalité et/ou capacité réduite) |
| | | - Applicatif - Maintenance inadéquate (mises à jour / correctifs non réalisés) |
| | | - Applicatif - Dégradation de la performance (fonctionnalité et/ou capacité réduite) |
| | | - Infrastructure - Maintenance inadéquate (maintenance régulière / réparations non réalisées sur les accès, les ascenseurs,...) |
| | | - Infrastructure - Dégradation de la performance (performance réduite / indisponibilité des accès, des ascenseurs,...) |

## Annexe 4 : Méthodologie d'évaluation du risque brut

### ✓ Survenance

L'approche méthodologique d'évaluation de la gravité du risque brut repose sur les principes suivants :

- ❑ Il s'agit d'une évaluation unitaire (analyse des évènements indépendamment entre eux) ;
- ❑ L'évaluation se situe à horizon un an (probabilité de survenance du risque dans l'année à venir).

La probabilité de survenance d'un risque correspond à la probabilité qu'il se réalise dans l'année à venir. On parle alors d'une probabilité d'occurrence à horizon 1 an.

L'évaluation de la probabilité de survenance se fait à partir de l'échelle de cotation suivante :

| Echelle de survenance | Faible | Moyenne | Forte | Très forte |
|---|---|---|---|---|
| Estimation | Peu probable | Probable | Très probable | Quasi certain |
| Echelle temporelle | Annuel | Trimestriel | Mensuel | Hebdomadaire |
| Volumétrie | Inférieur à 1% | 1% à 5% | 5% à 10% | Supérieur à 10% |

### ✓ Impacts

« En cas de survenance du risque, quels en sont les impacts ? »

Compte tenu de sa définition, le risque opérationnel est perçu comme entraînant systématiquement une perte financière. Or, les impacts générés par la survenance d'un risque ne transparaissent pas toujours dans les comptes. Il s'agit notamment du manque à gagner : des coûts d'opportunité (ex : souscriptions non réalisées du fait d'une erreur dans la documentation commerciale, …). De même, ces impacts ne sont pas uniquement d'ordre financier. Le risque peut agir sur la réputation de la Mutuelle, voir entraîner une sanction réglementaire.

| IMPACT | |
|---|---|
| | Faible |
| | Modéré |
| | Fort |
| | Critique |

A ce titre, 3 natures d'impact doivent donc être évaluées :

#### ➢ Financier

L'évaluation de l'impact financier s'effectue sur la base de l'échelle suivante :

| IMPACT FINANCIER | |
|---|---|
| Faible | [ 0 € ; 10 K€ [ |
| Modéré | [ 10 K€ ; 100 K€ [ |
| Fort | [ 100 K€ ; 500 K€ [ |
| Critique | [ 500K€ ; ∞ [ |

### ➢ Image / réputation

L'évaluation de l'**impact image/réputation** s'effectue sur la base de l'échelle suivante :

| IMPACT IMAGE / REPUTATION | |
|---|---|
| **Faible** | • Pertes / préjudices potentiels<br>• Quelques réclamations |
| **Modéré** | • Pertes / préjudices potentiels significatifs<br>• Nombreuses réclamations<br>• Assignations et saisine du médiateur |
| **Fort** | • Atteinte à l'image du secteur (publication dans la presse spécialisée) |
| **Critique** | • Atteinte à la réputation de la structure / des dirigeants<br>• Difficulté de conserver ou attirer de nouveaux clients<br>• Image sociale dégradée (ex : campagne de presse nationale) |

### ➢ Règlementaire

L'évaluation de l'**impact règlementaire** s'effectue sur la base de l'échelle suivante :

| IMPACT REGLEMENTAIRE | |
|---|---|
| **Faible** | Pas ou très peu d'impacts légaux et réglementaires. |
| **Modéré** | Emission par l'autorité réglementaire d'une demande de mise en conformité (Avertissement) nécessitant un changement de procédures. |
| **Fort** | Emission par l'autorité réglementaire d'une demande de mise en conformité (Blâme) nécessitant un changement important dans l'organisation ou les processus de l'entreprise. |
| **Critique** | Engagement de la responsabilité pénale (condamnation) des dirigeants de la mutuelle, possibilités de sanctions réglementaires (dont le retrait d'agrément) |

## • Annexe 5 : Famille de moyens de maîtrise

| Moyens de maîtrise niveau 1 | Moyens de maîtrise niveau 2 | Exemples |
|---|---|---|
| Facteurs d'atténuation | Documentation | Politiques, procédures, modes opératoires, règles de gestion, guides utilisateur, notes de service,... |
| | Organisation | Gouvernance, instances de pilotage, délégation |
| | Pilotage | Rapports, tableaux de bord, indicateurs clés,... |
| | Moyens humains | Compétence, formation, mise à disposition de ressources, expertises externes et/ou remplacement, développement de la polyvalence,... |
| | Veille | Veille juridique, réglementaire et technologique |
| | Assurance | Responsabilité civile, assurance multirisques des immeubles de placement et d'exploitation, assurance auto,... |
| | Plan de sécurité | Dispositif de sécurité des personnes et des biens, audit des installations,... |
| | Plan de continuité | PCA-PCI |
| Contrôles clés | Contrôles humains | Contrôles humains - manuels |
| | Contrôles informatiques | Contrôles informatiques - automatiques |

## • Annexe 6 : Critères d'évaluation des moyens de maîtrise

L'évaluation des moyens de maîtrise s'obtient par le croisement des 2 critères suivants :

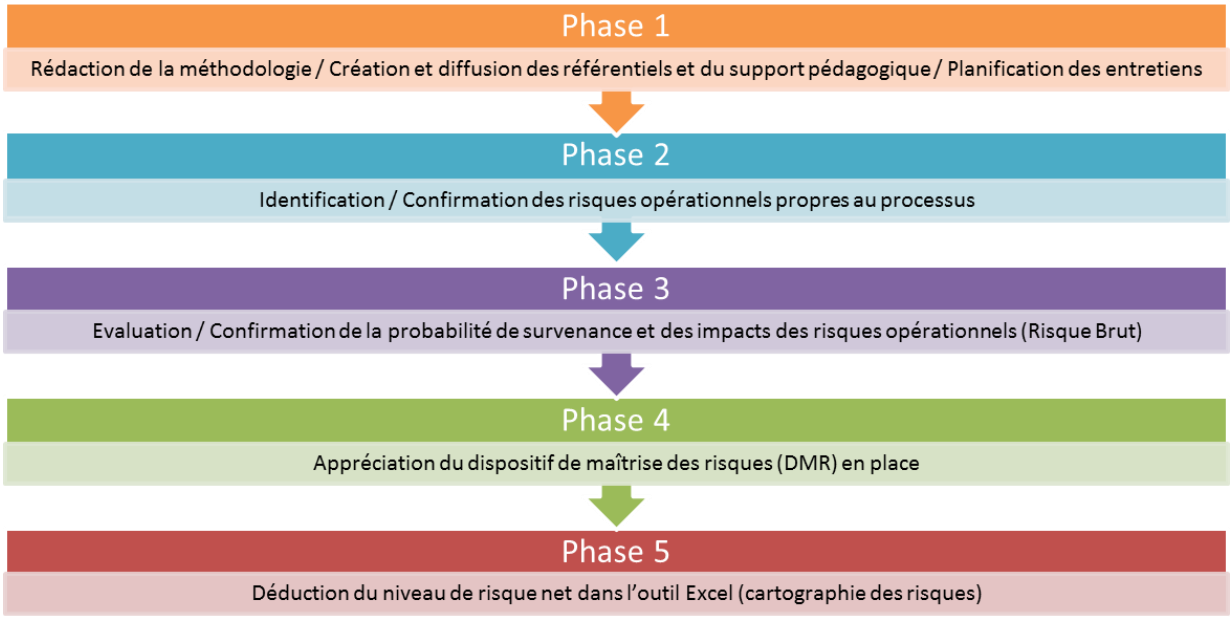
| | Echelle | Définition |
|---|---|---|
| Critères de formalisation | Non documenté, non traçable | - L'élément clé est effectué mais non décrit, non formalisé et impossible à vérifier |
| | Partiellement documenté, traçable | - L'élément clé est effectué et décrit, mais la traçabilité du contrôle n'est pas suffisante.<br>- L'élément clé est fait, traçable, mais sa documentation n'est pas suffisante. |
| | Documenté, traçable | - L'élément clé est formalisé, exploitable et vérifiable |

| | Echelle | Définition |
|---|---|---|
| Critères d'efficacité à couvrir le risque | Inefficace (efficacité < 25%) | - L'élément clé n'est pas effectué systématiquement ou pas du tout, ou le contrôle effectué n'aide pas à réduire le risque.<br>- Impact marginal sur la réduction du risque |
| | Partiellement efficace (efficacité entre [25%; 75%[ ) | - L'élément clé est parfois réalisé et aide partiellement à réduire le risque.<br>- Impact faible à moyen sur la réduction du risque |
| | Efficace (efficacité entre [75%; 95%[ ) | - L'élément clé est réalisé et couvre le risque suffisamment.<br>- Fort impact sur la réduction du risque. |
| | Très efficace (efficacité > 95%) | - L'élément clé est systématiquement réalisé et réduit la majeure partie le risque.<br>- Très fort impact sur la réduction du risque |

L'évaluation des moyens de maîtrise se lit directement dans la matrice suivante :

| | | Evaluation de l'efficacité | | | |
|---|---|---|---|---|---|
| | | Inefficace | Partiellement efficace | Efficace | Très efficace |
| | | efficacité < 25% | efficacité entre [25%; 75%[ | efficacité entre [75%; 95%[ | efficacité ≥ 95% |
| Evaluation de la formalisation | Non documenté, non traçable | Inexistant | Inexistant | Insuffisant | Significatif |
| | Partiellement documenté, traçable | Inexistant | Insuffisant | Significatif | Significatif |
| | Documenté, traçable | Inexistant | Insuffisant | Significatif | Très significatif |

## • Annexe 7 : Phases de l'entretien



## • Annexe 8 : Focus sur un processus précis

### ✓ Carte d'identité du processus

- **Processus concerné :** Achat et Vente d'Unités de Comptes (UC)
- **Responsable de processus :** Front Office
- **Finalités du processus :** Investir dans des fonds les capitaux en UC détenus par les adhérents
- **Données d'entrée :** carnet d'ordre transmis mensuellement par les équipes en charge de la gestion des contrats (Passif)
- **Documents et supports associés :** procédure et carnet d'ordres
- **Chiffres clés :** 550 K€ de cotisations en UC par mois

### ✓ Fiche des risques associés

- **Sélection des risques via le référentiel dédié**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Risque** | Risque niveau 1 | Exécution, livraison et gestion des processus | | | | |
| | Risque niveau 2 | Lacunes liées aux opérations de saisie, execution et suivi des opérations et des transactions | | | Risques relatifs à la diffusion de l'information et des données | Risques liés à l'externalisation au sens large |
| | **Risque niveau 3** | **Non-respect des délais et/ou des obligations envers un tiers / un client interne** | **Risque d'interface inter-services** | **Erreurs dans la saisie, le suivi ou le chargement des données** | **Données/informations erronées communiquées en interne** | **Mauvaise exécution des prestations fournies par le tiers au regard de l'attendu** |

- **Sélection des causes via le référentiel dédié**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Causes** | **Cause principale** | **Humain** | **Humain** | **Humain** | **Humain** | **Environnement externe** |
| | Cause secondaire | | Systèmes | | | |

- **Evaluation des risques bruts via la probabilité de survenance et les impacts**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Risque brut** | Probabilité de survenance | Forte | Forte | Forte | Forte | Forte |
| | Perte financière | Modéré | Critique | Critique | Critique | Critique |
| | Image / Réputation | | | | | |
| | Conformité réglementaire | | | | | |
| | Impact potentiel | Modéré | Critique | Critique | Critique | Critique |
| | **Criticité risque brut** | **Elevé** | **Majeur** | **Majeur** | **Majeur** | **Majeur** |

L'impact potentiel est uniquement financier mais selon le risque, l'impact est « Majeur » ou « Elevé ». La probabilité est Forte car ce processus ne s'effectue qu'une fois par mois. L'impact est Modéré pour le 1er risque car les pénalités de non investissement à payer à l'adhérent se comptent en % des primes investies. Pour les autres risques l'impact potentiel est « Critique » car les primes à investir mensuellement en UC sont supérieures à 500 K€.

- Evaluation des DMR et déduction des risques nets

| | | | | | | |
|---|---|---|---|---|---|---|
| | Documentation | Inexistant | Insuffisant | | Insuffisant | Très Significatif |
| | Organisation | | | | | |
| | Pilotage | | | | Insuffisant | |
| DMR | Moyens humains | | | | | |
| | Veille | | | | | |
| | Assurance | | | | | |
| | Plan de sécurité | | | | | |
| | Plan de continuité | | | | | |
| | Contrôles humains | | Significatif | Significatif | Significatif | Très Significatif |
| | Contrôles informatiques | | | | | |
| | **Evaluation globale DMR** | **Inexistant** | **Insuffisant** | **Significatif** | **Insuffisant** | **Très Significatif** |
| **Risque net** | | **Elevé** | **Majeur** | **Elevé** | **Majeur** | **Modéré** |

Pour ce processus fictif, il est nécessaire de mettre en place une documentation plus fournie et plus globalement de formaliser et augmenter le nombre de contrôles. Un document mensuel reprenant les contrôles clés de ce processus permettrait au Contrôle Interne de s'assurer de l'effectivité des contrôles.

- Annexe 9 : Interaction autour de la cartographie des risques opérationnels