Chapitre III

Les thématiques de risques opérationnels et le dispositif à mettre en œuvre

« *Au sein d'un cabinet de courtage, qu'il soit distributeur ou gestionnaire, nous allons retrouver un ensemble de risques opérationnels internes ou externes classiques à toute organisation. On a longtemps mis en œuvre des dispositifs de contrôle interne principalement intuitifs. En 2024, il est désormais nécessaire de gagner en formalisme, mais aussi de se professionnaliser avec des outils et méthodes usitées*. »

Un directeur d'une structure de courtage,
interviewé par l'auteur en 2024.

Le présent chapitre développe les enjeux clés de maîtrise des risques liés à l'activité du courtier. Sont ainsi détaillés de nombreux exemples opérationnels relatifs à la cartographie des risques, mais aussi aux enjeux de contrôle permanent. Des focus sur des risques opérationnels importants sont également mis en exergue.

Ce chapitre détaille les processus classiques du contrôle interne que sont :
– s'appuyer sur une cartographie des risques revue régulièrement ;
– s'appuyer sur une base de collecte des pertes et incidents ;
– s'appuyer sur un dispositif de contrôle interne intégrant notamment un plan de contrôle permanent permettant de sécuriser les risques opérationnels, mais aussi les risques de non-conformité.

À cela s'ajoutent d'autres sous-processus au titre de la sécurité de la donnée et de la continuité d'activité notamment.

Selon le niveau de maturité, il peut être pertinent d'outiller de telles démarches via des systèmes d'information de gestion des risques (SIGR) intégrant des modules d'audit, de contrôle interne, de cartographie des risques, de gestion des incidents, de continuité d'activité, et les reportings et plans d'actions associés à chaque module.

Le logigramme ci-après illustre la cohérence entre ces processus pour un courtier-délégataire de deux cents collaborateurs ayant décliné son dispositif de contrôle interne.

Dans cet exemple, il est intéressant de noter plusieurs points :

– le cabinet a outillé la démarche sur plusieurs des sous-processus et fait figurer dans son processus le recours à l'outil ;
– le cabinet de courtage appuie son dispositif de contrôle interne sur des référents métiers ;
– le fait de se doter d'un département dédié au contrôle interne, à la qualité et à l'organisation est aussi un facteur clé de succès ;
– le processus présente l'articulation des contrôles de premier niveau (lignes métiers) et de second niveau (département dédié) ;
– le courtier cherche à mesurer l'efficacité des contrôles réalisés et s'est fixé différents objectifs autour de son dispositif de contrôle interne, tels que la maîtrise des risques opérationnels, l'évitement des situations de non-conformité, mais aussi la protection des assurés.Comme l'évoque le directeur contrôle interne du cabinet interviewé en 2023 : « Nous avons mis en place un dispositif robuste fondé sur une formalisation des processus, mais aussi une structuration du contrôle interne dans laquelle le métier a un rôle clé à jouer. Cela a pris trois ans à mettre en place en partant d'un historique peu formalisé, mais dans lequel chacun connaissait son métier, ce qui nous a aidés. Cette formalisation et cet effort de structuration sont devenus indispensables à la faveur des audits de nos assureurs, mais aussi de l'ACPR. Nous avons recruté deux collaborateurs dédiés, ce qui représente un investissement important pour la société, mais on en retire des effets bénéfiques puisque cela permet d'être organisé pour répondre aux audits des assureurs et garantit peu à peu une meilleure culture de la traçabilité et de la maîtrise des activités. »

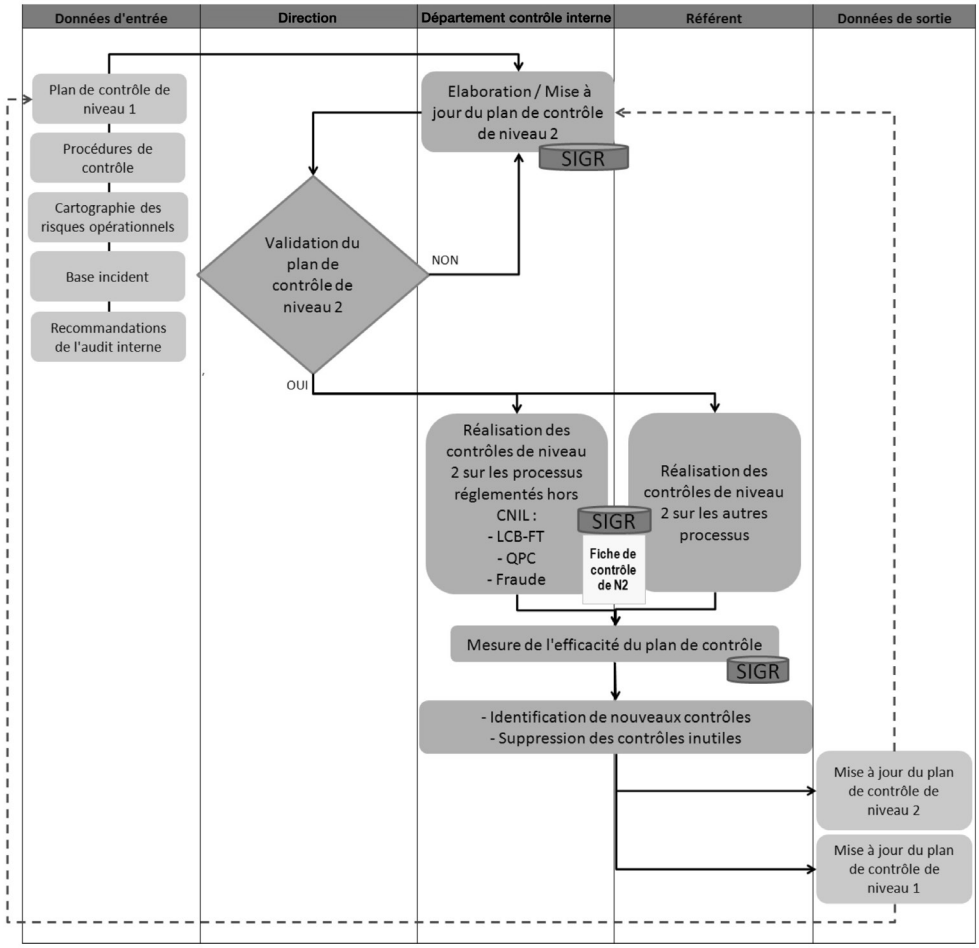
Acronymes associés : SIGR (Système d'information de gestion des risques), DOQCI (département organisation qualité contrôle interne), QPC (questionnaires protection de la clientèle).

Le suivi de performance de ce dispositif de contrôle interne s'est alors appuyé sur plusieurs indicateurs :

– le taux de conformité issu des contrôles sur les enjeux clés de conformité (LCB-FT, CNIL, DDA) et les plans d'action de remédiation associés issus des non-conformités détectées lors desdits contrôles ;

– le taux de maîtrise des risques sur les processus dits sensibles (adhésions, vie des contrats, sinistres, connaissance assurés) et les plans d'action de remédiation associés aux risques importants non encore maîtrisés à la suite d'un contrôle ;
– le nombre d'incidents par thématique et par type de risque (opérationnel, de non-conformité, financier), le coût desdits incidents et les remédiations associées ;
– le suivi des vingt principaux risques identifiés et évalués comme critiques pour la société, ainsi que les plans d'action sur les risques à mettre sous maîtrise (trois par an selon la politique de contrôle interne du cabinet qui doit prioriser ses ressources).

Figure 10. Logigramme d'un dispositif de contrôle interne d'un courtier d'assurance



Section I – La cartographie des risques

La cartographie des risques est un outil d'analyse de risque servant à différentes fonctions et est utile à la transversalité dans l'étude des risques.

La cartographie des risques intègre les risques passés, mais analyse aussi les risques présents et futurs, donnant un caractère de gestion globale au pilotage des risques.

I – Structuration et mise en œuvre, approche processus, risques, éléments de maîtrise

La cartographie des risques est à la fois une démarche méthodologique et un outil de représentation des futurs risques possibles. Elle n'est pas spécifique à l'entreprise de courtage. Cependant, elle devient de plus en plus une démarche normalisée demandée par différentes parties prenantes :

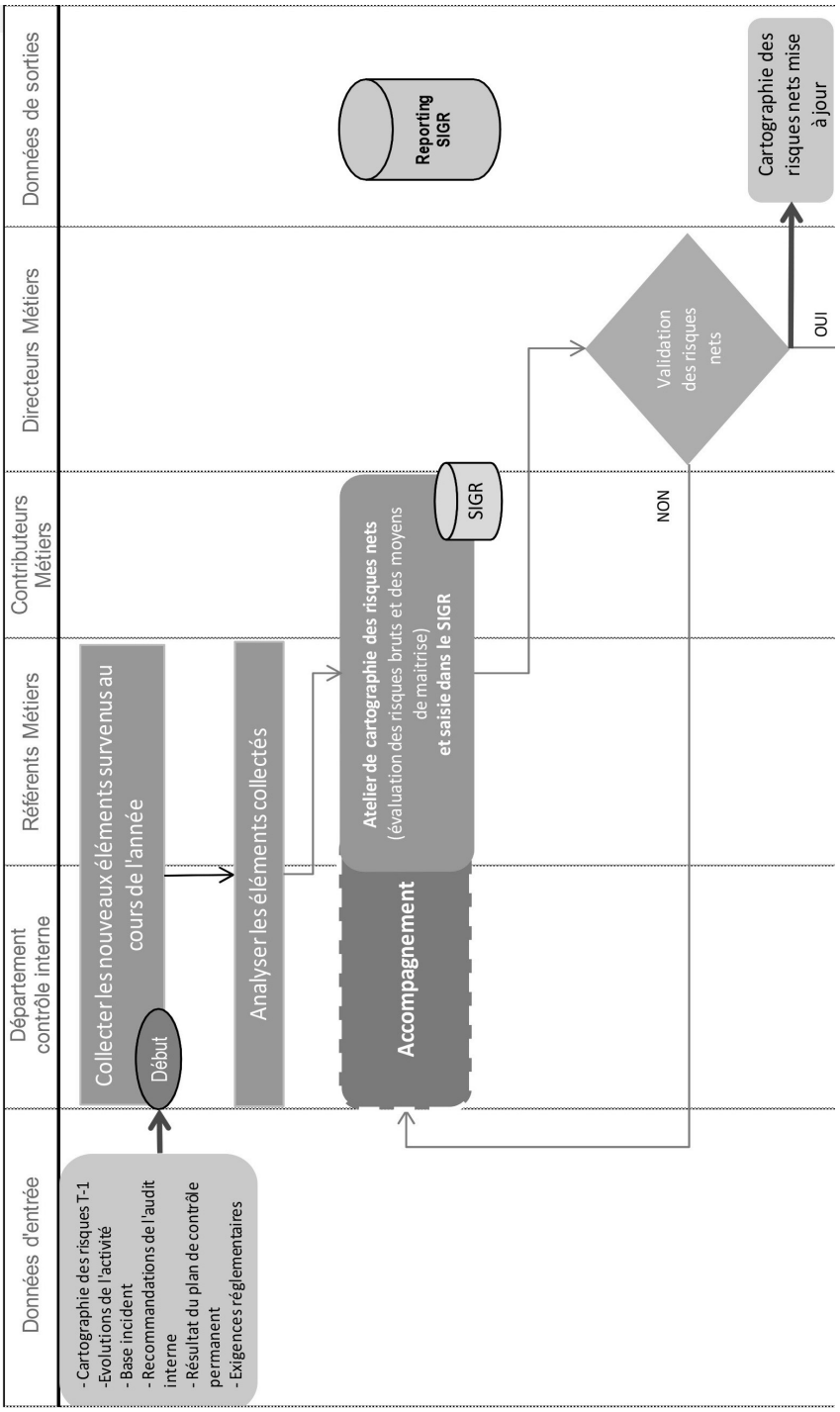
– les autorités de contrôle, cherchant à s'assurer que le courtier a mis en œuvre une démarche d'autocontrôle fondée sur l'approche par les risques ;
– les assureurs partenaires, voulant garantir la maîtrise de l'activité confiée en sous-traitance dans les conventions de distribution ou les conventions de délégation de gestion ;
– en interne, le courtier peut ainsi suivre ses principaux risques à piloter, sans chercher l'exhaustivité, et en gardant à l'esprit le principe de proportionnalité.

La cartographie des risques est un outil d'aide à la décision au service des responsables (membres de la gouvernance, mais aussi managers opérationnels). Initialement conçue comme un outil d'aide au pilotage des polices d'assurance (risques assurables, risques non assurables à traiter par des éléments de maîtrise du risque), la cartographie des risques est devenue une méthode très usitée de représentation et de formalisation de la réflexion et des décisions sur les risques dans les organisations.

La cartographie des risques est à la fois une approche méthodologique et un outil permettant de représenter les risques auxquels est exposée une organisation. Étudier ses risques via une cartographie, c'est se poser la question du pilotage de son activité en ayant une approche proportionnée des mesures à prendre selon les risques à piloter (Dufour, 2020). Réaliser une cartographie des risques, c'est à la fois se poser la question de ce qu'il peut advenir – les futurs risques possibles –, de ce qui peut concerner l'entreprise aujourd'hui – au moment de réaliser cet exercice –, mais aussi des risques survenus par le passé et pouvant encore concerner l'organisation aujourd'hui ou à l'avenir (les incidents). Cette approche est donc à la fois centrée sur la dimension temporelle, mais aussi la dimension spatiale : quels sont mes risques spécifiques à chaque site de production ?

Elle se présente en général sous forme de matrice et l'exemple de logigramme dans la Figure 11 ci-après détaille les approches classiques de revue des risques comme dans le cas de ce cabinet de courtage.

Figure 11. Logigramme de cartographie des risques d'un courtier de 200 collaborateurs



SIGR (Système d'information de gestion des risques), DOQCI (département organisation qualité contrôle interne)

À NOTER

Il n'existe pas une mais des approches variées pour réaliser la cartographie des risques. Si de bonnes pratiques ou des méthodes simples et complexes existent, la cartographie des risques est souvent spécifique à chaque organisation et vise à intégrer les particularités liées à sa stratégie, à son organisation et à ses processus, à ses projets passés, présents et futurs, mais aussi aux crises et incidents que celle-ci a traversés et qui ont pu contribuer à définir le cadre d'appétence au risque de l'entreprise, autrement dit les risques qu'une organisation et sa gouvernance souhaitent suivre, piloter et intégrer dans la cartographie des risques, approche formalisée d'aide à la décision.

La cartographie des risques est également une approche devenue, au fil des années, incontournable pour de nombreuses fonctions. Il peut s'agir de fonctions dédiées telles que les *risk managers* (gestionnaires de risques) qui cherchent à identifier, évaluer, prioriser et garantir le traitement et le suivi des principaux risques, les auditeurs internes qui cherchent à donner une assurance raisonnable sur le degré de maîtrise des processus, les commissaires aux comptes qui cherchent à s'assurer que les risques n'affectent pas la sincérité des comptes (en imposant parfois la prise en compte de provisions pour risques), mais également les autorités de contrôle (ACPR, CNIL, etc.) qui étudient la capacité des organismes contrôlés à respecter certains risques prévus par les lois et règlements et enfin par les membres de la gouvernance (conseil d'administration, direction générale, managers) qui ont besoin de prendre en compte la performance de l'activité, d'une part, et les risques pouvant porter à l'atteinte aux objectifs de l'organisation et donc à cette performance, d'autre part.

Les usages historiques de la cartographie des risques, tels que rappelés dans certaines sources de référence, sont les suivants :

– avoir une identification claire et concise des risques assurables ;
– connaître les principaux risques à piloter, sur la base d'une vision actualisée des incidents, des évolutions de l'activité et des risques inhérents.

Le principe de base de ces approches était de pouvoir recenser les risques, même simplement, de les analyser, d'étudier leur coût et de tracer les mesures mises en œuvre de détection, prévention, réduction, et ce, afin de négocier au plus juste les primes d'assurance dans le cadre de différents risques d'entreprises (responsabilité civile des mandataires sociaux, risques routiers, risques industriels, risques collaborateur clé, etc.).

Peu à peu, l'usage de la cartographie des risques a été aussi institutionnalisé par différentes réglementations ayant renforcé le recours, l'intérêt et les attendus en la matière. Ces usages concernent notamment des risques de non-conformité aux réglementations, telles que la loi Sapin II sur la prévention des risques de corruption et de conflit d'intérêts en 2016-2017, la loi de 2017 sur le devoir de vigilance rendant nécessaire la mise en œuvre d'une cartographie des risques dédiée, le Règlement général sur la protection des données de 2018. On peut encore citer les réglementations sectorielles (bancaires avec l'arrêté du 3 novembre 2014 sur le contrôle interne, et assurantielles avec la directive Solvabilité II) rendant obligatoire le fait de s'appuyer sur une approche par les risques. D'autres réglementations à venir (la directive CSRD, le règlement DORA sur la résilience cyber) rendent également essentiel le fait de s'appuyer sur une cartographie des risques.

L'augmentation des besoins issus des demandes d'audit (audit externe, audit interne) contribue également à faire de la cartographie des risques un incontournable de chaque mission d'audit sur des processus et activité.

L'évolution de la gestion des risques en tant que fonction et dispositif se traduit également par l'essor de ce que l'on appelle la gestion globale des risques, aussi appelée ERM (*Enterprise risk management*), soit un dispositif intégré à chaque processus et chaque décision favorisant la considération du facteur risque dans la prise de décision et mettant en tension le couple rendement/risque. L'idée de cette approche est que, sur chaque projet, chaque décision d'organisation, une analyse comparant opportunités et risques doit être réalisée en vue de définir le niveau d'appétence au risque que les décideurs sont prêts à prendre. Si les risques surpassent les gains escomptés ou que ces derniers sont trop difficiles à étudier, un choix de ne pas faire ou d'encadrement du risque par des mesures de détection, d'atténuation ou de prévention peut alors être décidé. Cette approche met la cartographie des risques au centre des enjeux, car elle en fait un outil incontournable pour se poser la question de l'acceptabilité des risques au regard des pertes et conséquences associées aux impacts de chaque risque et de la formalisation d'un cadre d'appétence, plus particulièrement pour les risques non assurables.

Le recours croissant à la cartographie des risques tend à se renforcer, preuve de l'utilité de cette dernière, véritable outil de pilotage et de suivi des risques.

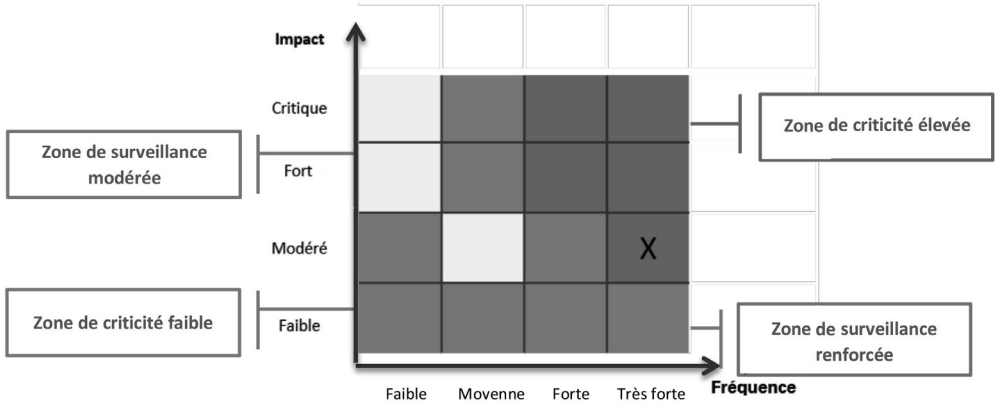
La cartographie des risques se représente généralement comme sur la Figure 12 ci-après, selon un modèle dit fréquence-coût rapprochant la probabilité de survenance du risque (nombre d'occurrences, parfois envisagé uniquement à dire d'expert en matière de vraisemblance) de ses impacts cumulés, ou en prenant l'impact le plus grave (impact humain, réputation, qualité, financier, réglementaire, continuité). Notons que la matrice la plus usitée internationalement est celle fondée sur l'approche fréquence-coût et représentant les cas par niveau sur chaque axe.

Le courtier devra alors se concentrer sur les risques en zone rouge – les principaux risques à piloter (en haut à droite), soit les risques à forte fréquence et aux impacts significatifs.

Quelques exemples de risque importants en cartographie pour un courtier :

– non-conformité RGPD causée par un traitement à risque ne faisant pas l'objet des mesures de maîtrise nécessaires : par exemple, dans le cadre de la délégation de gestion en prévoyance, le non-respect de la séparation des informations ne permettant pas d'assurer la conformité en matière de secret médical sera considéré comme une non-conformité majeure ;
– non-conformité en matière de protection de la clientèle : un courtier distribuera des produits d'assurance à des prospects ayant demandé à ne pas faire l'objet d'un démarchage commercial ;
– la fuite de données clients : un courtier aura fait l'objet d'un *phishing* avec fuite des données personnelles de ses assurés.

Figure 12. Exemple de cartographie des risques selon le modèle fréquence-coût



La cartographie des risques ne vise pas l'exhaustivité dans l'identification ou la description des modes de survenance d'un risque. Elle doit avant tout permettre d'obtenir un consensus interne sur les priorités de l'entreprise.

Notons que certains risques sont également obligatoires en matière de suivi, étant donné différentes réglementations : sécurité des biens et des personnes, risques industriels, risques de sécurité financière ou encore risques de cybersécurité par exemple.

Notons également que la cartographie des risques est une approche pour représenter le risque et sa survenance passée, présente, future : parfois, un tableau listant ces risques peut suffire. La matrice de cotation, telle qu'illustrée ci-dessus (Figure 12), trouve son utilité pour représenter une plus grande complexité en matière de risque. D'autres modes de représentation (par périmètre, en anamorphose par importance de chaque risque) peuvent également être usités.

Tableau 14. Logiques de maîtrise associées à la cartographie des risques

Logique de maîtrise des risques	Questions associées	Exemple
Risques à prévenir ou à anticiper	Des zones de risque sont-elles à anticiper au regard de tendance lourde du secteur ?	L'entrée en vigueur de nouvelles réglementations en matière de distribution ou de protection de la clientèle a-t-elle des impacts pour le cabinet de courtage et son activité ? (Le règlement européen DORA concernera les assureurs, mais aussi les courtiers à titre d'exemple avec la révision de la recommandation de l'ACPR sur le traitement des réclamations)
Risques déjà présents (potentiels)	Des zones de risque déjà présentes ne se sont pas encore traduites par des incidents, mais doivent être étudiées.	« Le cabinet de courtage a une conformité de 80 % sur les dispositifs DDA sur la base des trois derniers audits des assureurs partenaires. Un risque de non-conformité est cumulé au risque stratégique de fermeture de nos protocoles courtage en cas de non-remédiation de ces zones de risque sous un an. Une feuille de route doit être définie pour remédier aux non-conformités résiduelles dans le délai imparti, délai à l'issue duquel les assureurs partenaires réaliseront un audit de suivi. »
Risques déjà présents (avérés)	Des incidents (risques avérés) se sont produits au sein du cabinet : dispose-t-on d'une mesure d'impacts suffisamment précise et a-t-on mis en œuvre les mesures adéquates pour traiter l'incident lui-même et ses causes racines ?	Le cabinet a été confronté à une problématique de démarchage non souhaité d'un assuré par l'un des vendeurs. Ce dernier avait utilisé une liste non à jour, n'intégrant pas les dernières demandes de non-démarchage. L'informatique lui a transmis le fichier sans réaliser le contrôle associé. Un contrôle sous forme d'alerte fenêtre pop-up doit être mis en place pour s'assurer que tous les commerciaux ont bien fait les vérifications, et un contrôle croisé informatique-direction commerciale va être mis en œuvre.

Le tableau (Figure 13) ci-après présente les usages possibles de la cartographie des risques par fonction et par domaine. Nous précisons ensuite l'application qui peut en être faite par le courtier. Ces usages sont variés et peuvent être adaptés à la nature des conventions liant le courtier au partenaire assureur, mais aussi à la taille du courtier.