Forum des Compétences

Réflexions des établissements financiers

du

Forum des Compétences

Le risque résiduel, qui l'assume ?

Avec la contribution de

THALES

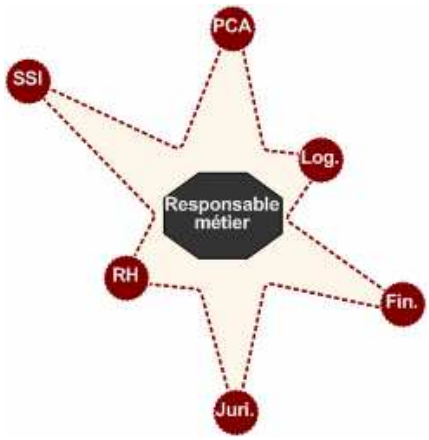
GROUPE DE TRAVAIL – FORUM DES COMPETENCES
LE RISQUE RESIDUEL : QUI L'ASSUME ?

Contexte

Afin d'assurer une maîtrise plus précise et efficace des risques, l'approche prudentielle des groupes de travail de la BRI – Banque des Règlements Internationaux - préconise de prendre en compte le risque opérationnel. Ainsi, selon la définition de Bâle II, on entend par risque opérationnel, « le risque de pertes dues à des personnes, processus ou systèmes défaillants ou résultant d'événements externes. Cette définition intègre en particulier le risque de non conformité». Cf. Accord Bâle II – Directive CRD.

Le responsable métier gère par nature l'ensemble des risques liés à son activité. Il gérait déjà les risques de contreparties, marché, liquidité, etc au sens de Bâle I et doit désormais prendre en compte le risque opérationnel au sens Bâle II.

Ainsi les institutions financières intègrent désormais la gestion du risque opérationnel dans la gestion quotidienne de leur activité métier. Le responsable métier se doit de prendre en compte ses risques opérationnels dans la conception et la mise en œuvre d'un nouveau produit ou d'une nouvelle activité



Dans ce contexte, il est primordial d'avoir une vision complète des risques impactant le métier et d'en déduire par conséquent les risques résiduels acceptés.

La multiplicité des expertises risques opérationnels (SI, juridique, humain, logistique, de conformité, sinistre externe, etc) tant en termes de fréquence que de sévérité des événements a nécessité la mise en place d'une gouvernance adaptée.

Cette réflexion a pour objectifs d'apporter des éclairages sur les points suivants :

- *Comment passer du risque au risque résiduel ?*
- *Comment consolider et évaluer le risque résiduel ?*
- *Qui l'assume ? Qui se charge de le suivre ?*

Comment passer du risque au risque résiduel ?

Le risque résiduel se définit comme étant le risque net après prise en compte des mesures, actions, dispositions… atténuants le risque brut. Il peut être obtenu après plusieurs itérations. Il peut être accepté ou non.

Lors de l'élaboration du nouveau produit ou service, une analyse de risque est réalisée.

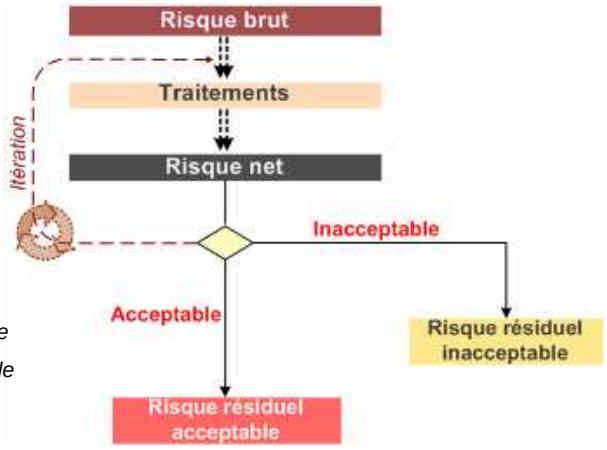


Figure 2. Le risque résiduel acceptable

Au cours de la phase de construction du produit, une appréciation préalable des risques afférents à ses activités est réalisée par différents experts (responsables de la continuité d'activité, ressources humaines, Sécurité des systèmes d'information, juridique, etc). Ce qui constitue la version initiale du dossier d'évaluation des risques.

Tout au long du cycle de vie du produit, ce dossier est régulièrement mis à jour.

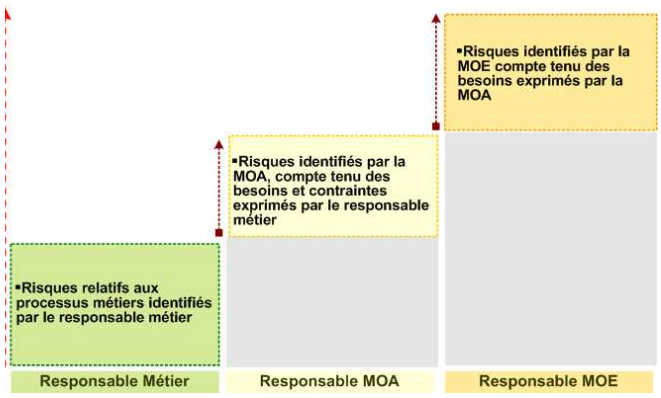


Figure 3.Cumul de quelques risques résiduels identifiés tout au long du cycle de mise en place et fonctionnement opérationnel

Un contrôle de 2e niveau est assuré par une fonction d'analyse des risques et des processus, indépendante (exemple risk manager, contrôle permanent) qui a une bonne connaissance des activités métier. Elle a pour mission d'émettre un avis sur les risques évalués par les experts de chaque activité et de le communiquer ensuite au responsable métier. Pour ce faire, il est nécessaire que les experts expriment leurs analyses dans un langage orienté métier. La consolidation de ces analyses constitue le *dossier d'évaluation des risques*. En effet, il permet au responsable métier d'avoir une vision globale des risques résiduels qu'il a acceptés.

En phase de mise en œuvre du produit ou du service, le responsable métier doit s'assurer de la mise à jour du dossier d'évaluation des risques. Ce processus de mise à jour doit être également documenté.

L'évaluation des risques doit être révisée de manière périodique dans le but de tenir compte de l'évolution de l'environnement réglementaire et technique, du changement des périmètres métier ou organisationnel et de l'apparition de nouvelles menaces.

Deux familles de risques sont à distinguer :

- Les risques *courants* inhérents à l'activité mais avec un impact limité sur le processus métier (exemple : fraude quotidienne liée aux cartes bancaires, pertes/vol des cartes, etc). Ces sinistres récurrents sont traités comme des pertes opérationnelles et pris en compte dans les budgets relatifs à chaque métier.
- Les risques *exceptionnels* ont une probabilité d'occurrence faible et un impact très fort sur le fonctionnement du process métier (fraude exceptionnelle, indisponibilité des réseaux, sinistre majeur, choc extrême, etc). Ces risques font partie intégrante du calcul des fonds propres.

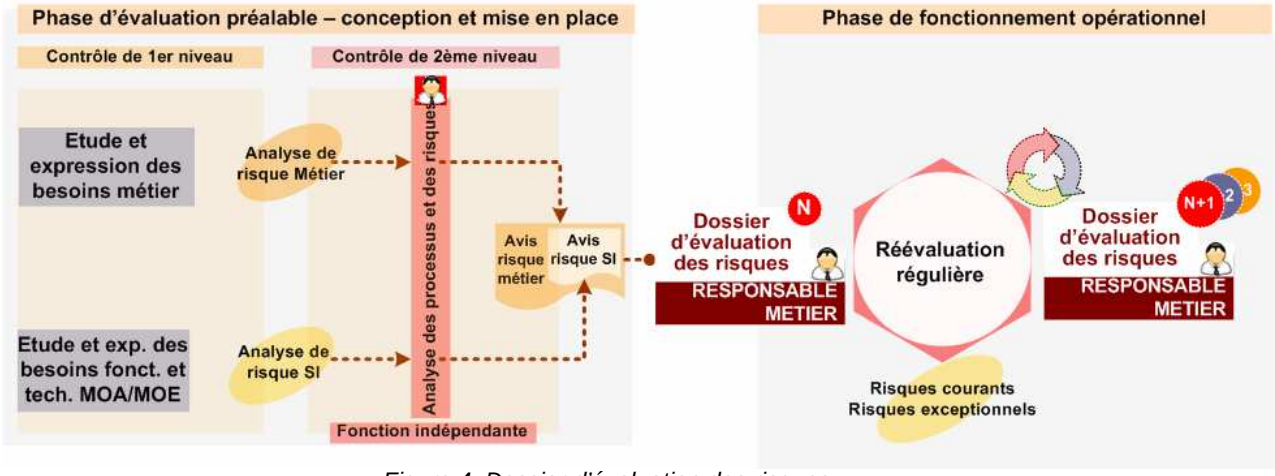


Figure 4. Dossier d'évaluation des risques

En résumé, le dossier d'évaluation des risques est un outil de pilotage du responsable métier. Il lui permet de regrouper l'ensemble des risques identifiés, tout au long de la phase de conception et de mise en œuvre; de les quantifier en vue de les prendre en compte dans l'estimation des pertes opérationnelles et le calcul du capital économique (Bâle II); et de pratiquer les arbitrages et les investissements nécessaires.

Exemple de constitution d'un dossier d'évaluation des risques à partir du standard ISO 27005

Parmi les approches les plus communément admises, la norme ISO 27005 – risk management, expose la démarche d'appréciation et de traitement des risques.

Cette méthode peut être utilisé par l'ensemble des experts sur lesquels s'appuie le responsable métier pour la constitution de son dossier d'évaluation des risques et se décline de la manière suivante :

- **Etape 1 - Etablissement du contexte** : consiste à spécifier le périmètre de l'appréciation des risques, l'environnement et l'organisation du processus métier.
- **Etape 2 - Appréciation du risque** : se décompose en deux sous parties :
  - L'analyse des risques : identifie et quantifie les actifs sensibles, les menaces et vulnérabilités et estime, la probabilité d'occurrence des risques identifiés en vue de calculer les risques.
  - L'évaluation des risques : permet de classifier les risques au regard des critères d'évaluation, préalablement établis par les objectifs et contraintes imposés par le responsable métier.

- **Etape 3 - Traitement du risque :** consiste à décider des solutions à envisager selon les options suivantes : refus/évitement, transfert du risque, réduction du risque et prise de risque.
- **Etape 4 - Acceptation du risque** : permet d'apprécier le risque résiduel obtenu une fois que le traitement du risque est mis en œuvre. A cet égard, le responsable prend la responsabilité d'assumer son risque résiduel ou d'arrêter le projet.

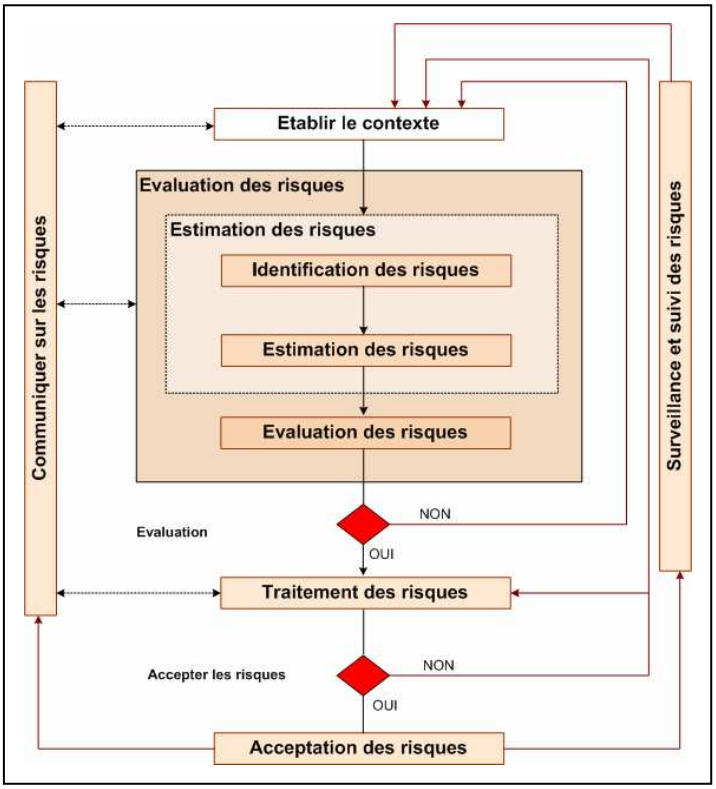


Figure 4.Source : schéma de l'iso 27005

En conclusion, le responsable Métier assume son risque résiduel au travers le processus de consolidation du dossier d'évaluation des risques. Il s'appuie sur :

- Les experts qui l'accompagnent dans la qualification et le traitement des risques,
- Les fonctions de gestion des risques et de contrôle.

Pour que ça fonctionne, il est indispensable d'avoir une gouvernance adaptée à la culture et au niveau de maturité de chaque établissement.

Composition du Groupe de travail

- **Marouen BELLAZRAK, Thales**
- **Carine CABALO-SIARRI, La Poste**
- **Marc DEVALLIER, La Banque Postale**
- **Wilfrid GHIDALIA, Forum des Compétences**
- **Gilles MAWAS, BNP Paribas**
- **Jean-Philippe REGIN, Thales**
- **Jacques SARRASIN, LCL**