Septembre 2017

Gestion du Risque Opérationnel

Group Risk Management
Sylvie HULIN
Rémy BAGUE

Journées d'études de l'Institut des Actuaires et du S.A.C.E.I
Club ERM
Deauville - Vendredi 22 septembre 2017

Sommaire

Quelques définitions et limites

Définitions

- **Directive Solvabilité 2**
  - Article 13 (33) – Le risque opérationnel est défini comme le risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs;
  - Article 101 (f) Le risque opérationnel visé au premier alinéa, point (f) comprend les risques juridiques mais ne comprend ni les risques découlant des décisions stratégiques, ni les risques de réputation.
- **Bâle 3**

Le risque opérationnel, […], représente en moyenne 15% du capital minimum requis.

Exemples d'ambiguïtés

- **Risques de réputation et risques stratégiques**

Ils sont exclus de l'exigence de modélisation, mais il n'est pas précisé s'ils doivent être pris en compte dans le système de gestion du risque opérationnel.

- **Réglementation et fiscalité**

La réglementation ou la fiscalité peuvent-elles être considérées comme des évènements extérieurs et être ainsi considérées comme du risque opérationnel ?

Quelques exemples de problématiques

Frontières

En tant que gestionnaire de risques, l'objectif est de s'assurer que l'ensemble des risques sont bien pris en compte et une seule fois. Cependant, il peut être parfois difficile de déterminer la catégorie lorsque les risques se situent à la limite entre deux catégories.

- **Exemples**: taxes (est-ce un risque opérationnel ?), risque de modèle ou risque de tarification (sont-ils des erreurs ou doivent-ils être identifiés dans une catégorie de risque à part ?), risque de souscription (à quel moment le risque de souscription devient-il un risque opérationnel ?), provisions techniques (sont-elles économique ou comptables ?).

Effet « multiplicatif »

L'effet multiplicatif correspond à la survenance concomitante de plusieurs scenarios petits ou moyens. Cette accumulation pourrait engendrer des pertes plus importantes que le cumul des pertes individuelles.

- **Exemple 1:** la mise à jour d'un système informatique prend du retard, et la publication de documents réglementaires est différée générant des amendes. Une attaque cyber sur ce système, ou la perte d'une personne clé dans le projet à ce moment là, ayant en soit un impact marginal, aurait dans ce cas un effet amplifié.

- **Exemple 2:** le déménagement d'une filiale menant à la perte de compétences, notamment dans le domaine de la gestion des sinistres, combinée avec une hausse des coûts des dommages corporels préjudices corporels en assurance auto, ont conduit à la mise en liquidation de la filiale en question.

A chaque type de structure doit correspondre son approche

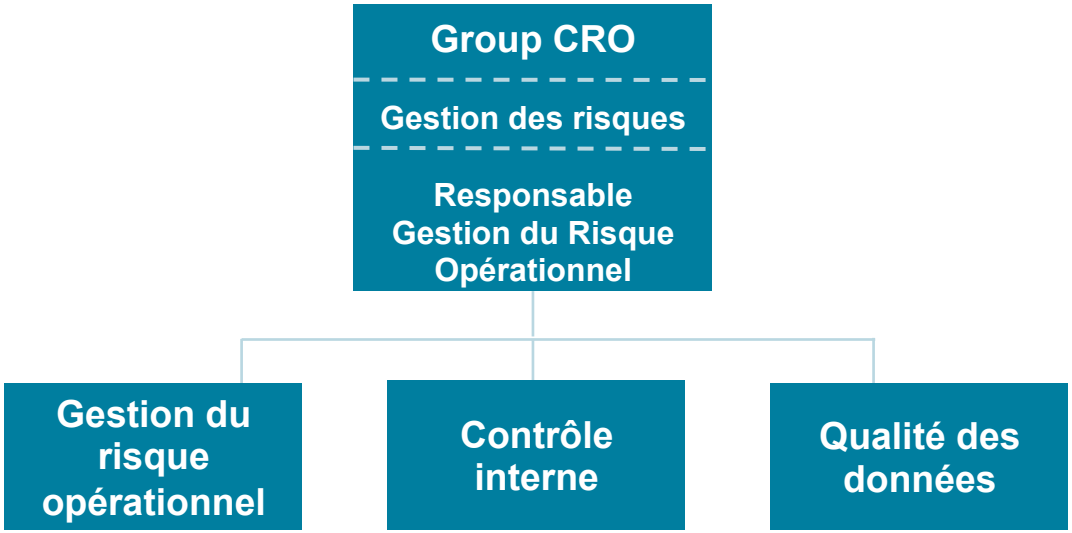
Réassureurs		Banques et assureurs
• La réassurance a été officiellement réglementée depuis 2005 dans l'Union Européenne[1)] • Les exigences en matière de réglementation sont spécifiques concernant le risque opérationnel	**Expérience réglementaire** **Récent** / **Oui**	• Les banques sont réglementées depuis plus de 100 ans avec des changements significatifs dans les années 80 • Le risque opérationnel est au cœur du sujet depuis le Comité de Bâle en 1998
• Petites entreprises • Grandes entreprises internationales	**Ressources dédiées** **Moins** / **Oui**	• Les banques emploient généralement plusieurs dizaines de milliers de collaborateurs • Les opérations de banque de détail sont principalement effectuées dans le pays du siège social (ceci peut être différent pour les services bancaires aux entreprises)
• Processus complexes essentiellement basés sur le niveau d'expertise • Une large gamme d'activités indépendantes	**Homogénéité des processus** **Non** / **Oui**	• Augmentation et industrialisation des processus de base • Effet d'échelle important
• Business model : B to B	**Réseau de clients contraignants** **Non** / **Oui**	• Business model : B to C

Ces différences de structures et d'opérations, renforce la gestion du risque opérationnel des réassureurs sur l'analyse d'évènements individuels spécifiques, plutôt que sur des évènements de fréquence. Elle nécessite le développement de techniques innovantes de surveillance.

1) Directive 2005/68/CE du Conseil du 16 novembre 2005 relative à la réassurance

Sommaire

Organisation de SCOR pour la Gestion du Risque Opérationnel



- L'organisation de l'équipe a pour objectif de garantir une association efficace et pertinente de tous les mécanismes de la gestion du risque opérationnel.
- Le système de contrôle interne vérifie que des contrôles pertinents soient correctement définis et effectifs pour réduire la probabilité d'occurrence des risques, ainsi que leur coût.
- La qualité des données a pour objectif notamment, que les données utilisées pour modéliser les risques correspondent bien à l'exposition réelle.

Le cadre de gestion du risque opérationnel de SCOR donne une représentation synthétique de l'ensemble des sujets

Thèmes	Catégories	Commentaires
Fraude	Externe	
	Interne	
Conformité	Blanchiment d'argent	
	Lutte anti-corruption	Notamment dans la plupart des processus de paiement
	Sanctions & Embargo	Inclut les lois anti-trust
	Mauvaises pratiques	Non-respect des règles et usages des pratiques commerciales
	Cadre réglementaire	Toute violation ou faute pour lesquelles SCOR pourrait être condamnée à une amende ou effectuer de nouveau un travail prenant en compte les aspects juridiques et de conformité
Gouvernance	Comités	Efficacité des comités
	Politiques	Corpus des politiques de fonctionnement et des guides opérationnels
Juridique	Commercial	Tout nouveau risque provenant d'une activité de sous-traitance
	Groupe	
Données	Qualité	La qualité des données a un impact sur la cohérence et la pertinence des résultats. Intégrité, disponibilité & confidentialité sont liées à la conformité et à la réputation.
	Intégrité	
	Disponibilité	
	Confidentialité	
Cyber		
Production	Continuité	Plan de Continuité d'Activité
	Efficacité	Efficacité liée aux budgets et coûts cachés
	Actes malveillants	Tous dégâts portés aux actifs de SCOR ou à ses moyens de production
	Etats financiers	Risques reliés liés aux processus d'établissement des comptes financiers
	Erreurs humaines	
Ressources Humaines	Recrutements	Régulation, contrôles systématiques, processus, efficacité
	Salaires	Transparence, éthique/principes, récompenses
	Formations	Motivation, amélioration de la connaissance et des compétences
Réputation	Commercial	Franchise: Capacité à attirer et fidéliser les clients et investisseurs
	Groupe	Capacité à attirer et fidéliser les collaborateurs
Projets	Interne	Projets en échec ou coûts supplémentaires non justifiés
	Sous-traitance	

Le cadre de SCOR s’appuie sur quatre principes fondamentaux

- **Complétude**

Garantie que tous les aspects du risque opérationnel sont bien pris en compte. Les redondances peuvent être gérées lorsqu’elles sont identifiées.

- **Visibilité/profondeur**

Permet que les informations et données soient pertinentes, et donnent ainsi aux directions opérationnelles les éléments nécessaires à l’amélioration de l’organisation aux bons niveaux.

- **Flexibilité**

L’environnement opérationnel, tant commercial qu’organisationnel, évolue rapidement. Le cadre doit donc offrir la possibilité de s’adapter aux changements ainsi qu’au point de vue de la direction.

- **Cohérence**

Les rapports réglementaires et les différentes entités opérationnelles nécessitent de produire de l’information sous différents formats, avec plusieurs niveaux de granularité et de prise de décision concernant le risque opérationnel. Par conséquent, un cadre cohérent est essentiel pour maintenir l’efficacité et répondre aux priorités.

Exemples de facteurs de réduction des risques

- **Gouvernance**

Les comités, les politiques et les lignes directrices contribuent à diffuser une culture du risque opérationnel. Les définitions des principes permettent d'accorder la compréhension des concepts, et des actions de réduction du risque opérationnel.

- **Contrôle interne**

La plupart des activités de SCOR et les contrôles des risques associés à ces activités sont documentés et suivis.

- **Systèmes et outils dédiés**

Mécanismes de sécurité informatique, outils de lecture de documents, outils analytiques automatisés, projets orientés sur les données c'est-à-dire sur la qualité et la sécurité des données.

- **Culture du risque**

Les sujets liés au risque opérationnel sont régulièrement présentés au conseil d'administration de SCOR. Des exemples concrets, « risk tales », sont développés et présentés à l'ensemble de la société. Le personnel suit régulièrement des formations sur les sujets de conformité, et une communication régulière sur les tentatives et méthodes de fraude est effectuée.

- **Audit interne**

Toutes les activités peuvent être contrôlées afin de vérifier que les opérations et les contrôles sont correctement effectués. Proposition d'axes d'amélioration ou d'éventuelles corrections.

- **Transferts de risque**

Acquisition de couvertures d'assurance afin de protéger SCOR de certains risques opérationnels (Responsabilité civiles des mandataires, Cyber …)

Exemple de suivi du risque opérationnel au niveau du Board

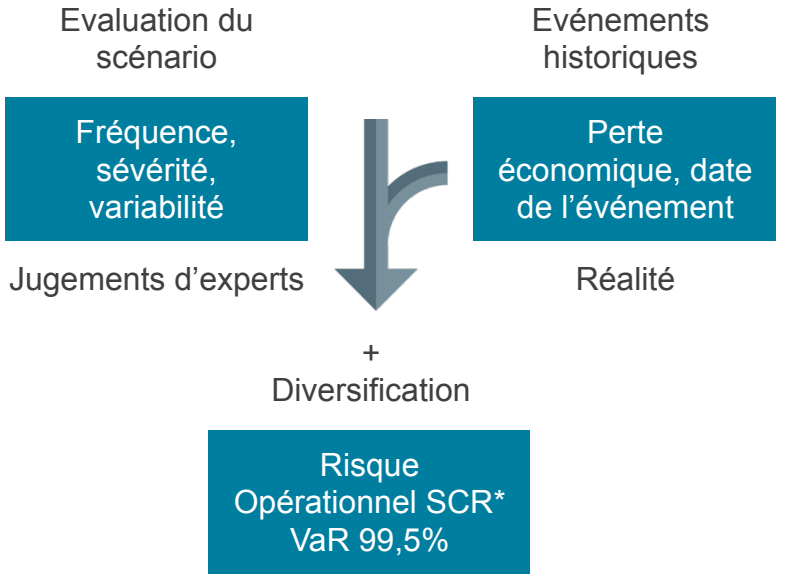
- Forte implication de la direction qui s'appuie sur des rapports trimestriels synthétiques.
- Un modèle interne de gestion du risque validé permet à SCOR de prendre en compte des scénarios décrivant l'exposition actuelle et de potentiels futurs scénarios.
- Une évaluation du contrôle interne à l'échelle du groupe fournit à SCOR un statut sur les risques et les contrôles liés aux processus.
- Un tableau de bord dédié au risque cyber donne un aperçu de l'évolution de la menace externe, de l'exposition de SCOR et de l'amélioration de la cyber sécurité.

L'évaluation des risques opérationnels repose à la fois sur des scénarios et sur des incidents historiques

Root Causes
Changement du contexte juridique, réglementaire et commercial
Litiges Commerciaux et Contractuels
Fraude Externe
Fluctuation de la charge de travail
Erreur Humaine
Fraude Interne
Risque de Conformité Juridique et Réglementaire
Perte d'effectif
Acte Malveillant
Nouvelle entité/ Ligne d'activité/ Département
Défaillance d'un système
Indisponibilité des bureaux

Domaines d'activités
Comptabilité
Gestion d'actifs
Sinistres Life
Sinistres P&C
Tarification Life
Tarification P&C
Réserves Life
Réserves P&C
Rétrocession Life
Rétrocession P&C
Trésorerie
Souscription Life
Souscription P&C

Modèle de risque opérationnel



- Les **root causes**, ou causes premières, sont les sources potentielles de scénarios opérationnels. A titre d'exemple, une inondation n'est pas explicitement répertoriée en tant que cause principale mais elle peut déclencher une indisponibilité de bureaux ou une panne de système.
- Les **domaines d'activité** sont configurés pour correspondre à l'organisation de SCOR. Ils doivent être compris comme toutes les activités sous jacentes à ces domaines d'activité. Par exemple, la souscription P&C rassemble tous les processus qui contribuent à une décision concernant celle-ci.

Le modèle interne de risque opérationnel permet d'améliorer la gestion du risque sur plusieurs plans

Evaluation du scénario

- **Diffusion de la culture du risque**: le processus d'évaluation des scénarios permet un partage d'idées, de comparer les risques et de mieux comprendre les phénomènes conduisant aux pertes.
- **Plus grande implication des opérationnels**: mieux prendre en compte les risques et les spécificités des processus opérationnels. Il peut y avoir, en effet, un risque que l'exercice d'évaluation soit purement théorique.
- **Décloisonnement des silos:** lors des ateliers d'évaluation de scénarios, plusieurs personnes provenant de différents domaines d'activités ont été invitées à partager leurs points de vue, à comprendre et à profiter d'expériences alternatives pour éventuellement compléter les scénarios.

Gestion des incidents

- **Contexte**: SCOR ne subit qu'un taux réduit d'incidents significatifs. L'amélioration de leur gestion est clé pour accroitre la maîtrise des incidents à travers le Groupe.
- Amélioration de la gouvernance de la gestion des incidents et des bases de données (évaluation et gouvernance)

Meilleure compréhension des composantes du risque

- L'évaluation des risques opérationnels reste récente dans l'histoire des modèles de risque. Les résultats du modèle ouvrent un large éventail d'études théoriques afin de mieux comprendre les différentes composantes des risques opérationnels.
- SCOR a notamment amélioré sa compréhension des corrélations au sein des risques opérationnels (corrélation, causalité, dépendance) et entre le risque opérationnel et d'autres risques (définition des facteurs causaux, interactions entre les autres modules d'évaluation des risques).

SCOR développe plusieurs utilisations de son modèle

Classement des risques

- Le modèle fournit des résultats par type de risque opérationnel qui sont ensuite alloués par entités juridiques. Cela fournit une vision pertinente des points sur lesquels la direction doit s'orienter afin d'atténuer ou minimiser les risques.
- Les résultats font aussi l'objet de discussions pour s'assurer qu'ils correspondent à une réalité.

Impact des actions atténuantes

- **Gestion de l'exposition**

SCOR définit dans le plan stratégique actuel comme objectif stratégique de minimiser le risque opérationnel. Une mesure d'exposition appropriée pourrait être la perte à 200 ans (ou VaR 99,5%) fournie par le modèle de risque opérationnel.

- **Optimisation Coût-Bénéfice**

Les résultats du modèle peuvent aider à l'identification des zones où le risque opérationnel résiduel peut être encore réduit. Par exemple, par des contrôles renforcés ou des mécanismes de transfert de risque (assurance). Le coût de ces mesures peut ensuite être comparé au gain de coût du capital pour aider à prendre une décision de mise en œuvre de ces mesures.

- **Exemples d'application:** couverture d'assurance cyber, amélioration des outils de tarification, évaluation des projets.

Néanmoins, le modèle présente certaines limites

- **Une vision alternative**

Les données d'entrées et les résultats du modèle doivent être revus afin de s'assurer qu'ils correspondent à une réalité. Le modèle est conçu ou calibré sur un univers des risques à un moment donné. Par la suite, il est donc nécessaire de s'assurer que le modèle est toujours pertinent sur un univers fluctuant. Afin de pouvoir identifier les déviations potentielles du modèle, il est donc nécessaire d'avoir, une vision alternative des risques, potentiellement qualitative.

- **Transparence**

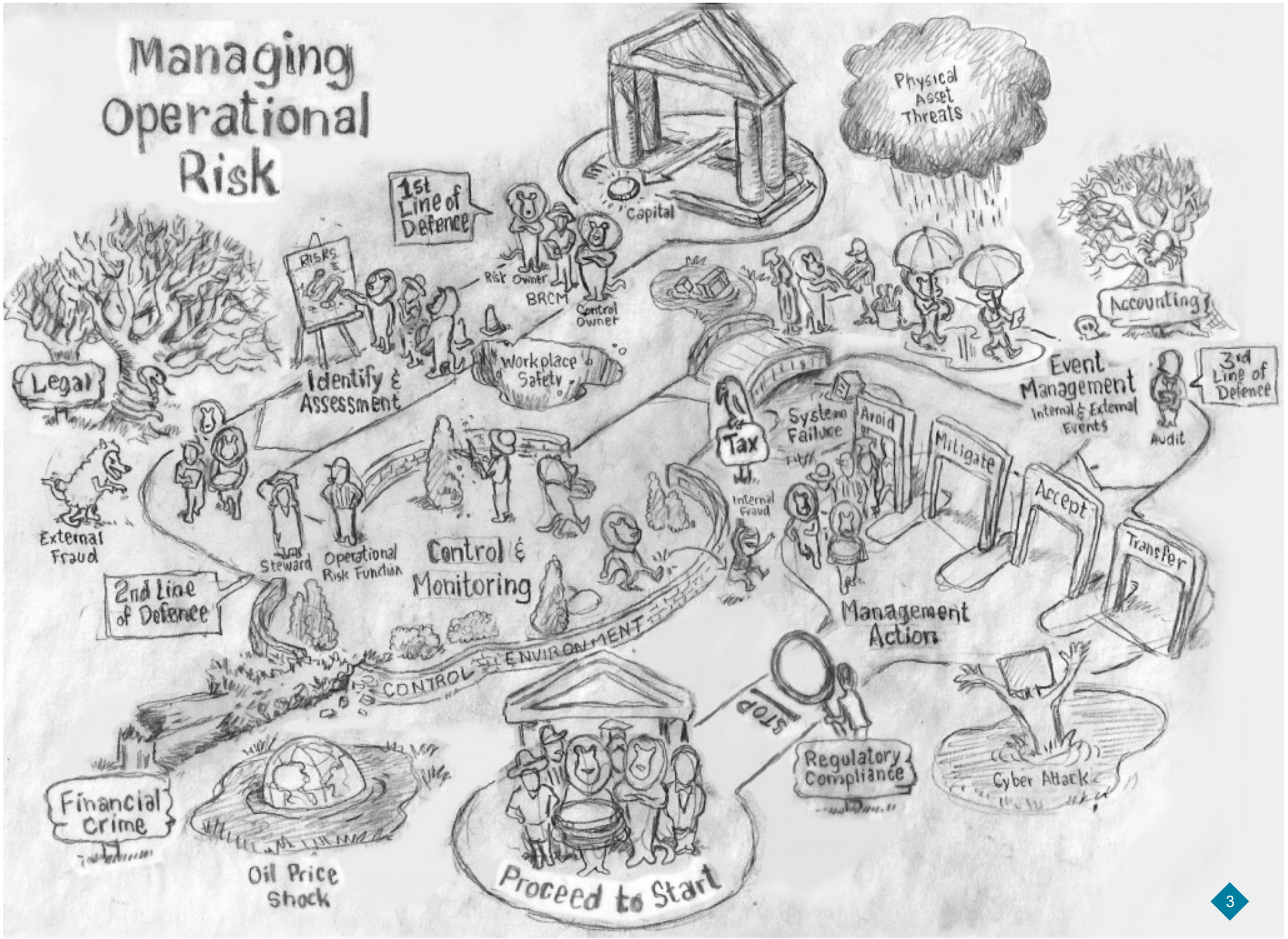
Il existe un équilibre entre, d'une part, une transparence forte sur le modèle, ses résultats, les explications sur son fonctionnement afin de fournir des données pertinentes et conserver un jugement pertinent sur l'analyse des résultats ; et d'autre part, éviter le protectionnisme pour empêcher les contributeurs d'ajuster les données afin de piloter les résultats.

- **Application**

Au moment de l'établissement des scénarios, les contributeurs ne voient pas l'impact de leurs scénarios sur les résultats du modèle. Ceci évite qu'ils soient influencés par les résultats. Cependant, les résultats finaux leurs sont communiqués pour assurer une cohérence générale.

Sommaire


ESSENTIALS OF RISK MANAGEMENT:
1. DON'T DO ANYTHING WRONG TODAY.
2. DON'T DO ANYTHING WRONG TOMORROW.
3. REPEAT.
Complex Discovery
GLASBERGEN
© Randy Glasbergen / glasbergen.com


Managing Operational Risk
1st Line of Defence
Capital
Physical Asset Threats
Risks
Risk Owner
BRCM
Control Owner
Accounting
Legal
Identify & Assessment
Workplace Safety
Event Management
Internal & External Events
3rd Line of Defence
Audit
Tax
System Failure
Avoid
Mitigate
Accept
Transfer
Internal Fraud
External Fraud
Steward
Operational Risk Function
Control & Monitoring
2nd Line of Defence
Management Action
CONTROL ENVIRONMENT
STOP
Regulatory Compliance
Cyber Attack
Financial Crime
Oil Price Shock
Proceed to Start

Défis liés à la communication des risques opérationnels

- **Risque non rémunéré**

En d'autres termes, il n'y a pas de récompense pour les incidents évités, et donc aucune incitation financière directe à la prudence. Les mesures de prudence devraient donc logiquement être obligatoires et peuvent donc être un frein à la culture. Il y a donc une approche équilibrée et raisonnable à trouver pour diffuser cette culture du risque, mais qui nécessite parfois de nager à contre courant.

- **Fonctionnements en silos**

Le risque opérationnel est transversal et de nombreux processus sont en partie liés entre eux.
De plus, des corrélations existent entre les différents domaines d'activité pour lesquels la communication dans la gestion des risques serait pertinente.
Plus ces domaines sont spécialisés, plus cette communication est difficile.
Exemple: la fraude et le risque cyber.

- **Risques oubliés**

Risques d'une telle évidence qu'ils ne sont pas mentionnés et pour lesquels on considère qu'ils sont correctement gérés par des équipes dédiées.
Exemple: sécurité physique des employés.

- **Risques cachés**

Risques intentionnellement non mentionnés afin d'éviter toute charge de travail supplémentaire visant à y remédier, ou toute accusation sur une possible mauvaise gestion.
Exemple: préciser des erreurs de programmation dans des outils.

- **Risques sensibles**

Risques connus mais complexes et donc évités car la prise en compte serait trop lourde.
Exemple: les risques sociaux liés à une dégradation des conditions de travail.

Développer une communication efficace pour diffuser la culture du risque: retour aux bases

- **Objectif**

L'objectif principal de la communication sur les risques consiste à les atténuer. La définition d'un objectif clair est nécessaire pour éviter des effets contre-productifs.

Exemples d'objectifs ciblés:

- Améliorer la connaissance du risque
- Mieux sensibiliser au risque
- Fournir une meilleure visibilité aux départements des risques
- Encourager le personnel à utiliser de manière spécifique un outil de gestion du risque
- Accéder à de nouvelles ressources d'expertise pour l'analyse des risques

- **Fréquence**

La fréquence est également un élément clé. La multiplicité des formes et des sujets de communications peuvent faire entrer les différentes communications en compétition. Cela peut conduire à une dilution complète des message centraux. D'un autre côté, une fréquence trop faible prête le message à l'oubli.

Par conséquent, en fonction de l'exposition au risque et de l'objectif recherché, la fréquence et la priorité de la communication doivent être correctement définies et modulables.

- **Différence et équilibre entre la communication et la formation**

Parfois, les risques évoluent rapidement et il y a peu de contenu pour la formation, mais communiquer sur le risque et appeler à la vigilance peut faire partie d'une campagne de communication.

Exemple: cyber, fraude, Plan de Continuité d'Activité (PCA), corruption, sous-traitance.

Exemple de communication chez SCOR: les « Risk Tales »

- Le département de gestion des risques développe des cas d'étude basés sur les incidents survenus dans d'autres entreprises. En particulier les cas d'assurance, mais certains incidents non liés à l'assurance sont également pris en compte.
- Les analyses et les exemples sont étudiés par les gestionnaires de risques des différentes filiales dans le but de recueillir des données d'ensemble, de défaillance globale mais également d'impact sur les marchés locaux.
- Ces cas sont utiles pour sensibiliser au risque, capitaliser sur l'expérience acquise et approfondir les propres analyses du groupe.
- L'objectif des cas d'étude est de:
  - **Développer la culture du risque à travers tous les départements de SCOR**
  - Améliorer **la prise de conscience**
  - **Former le personnel** sur les principes de la gestion du risque en se concentrant sur **les leçons tirées** des incidents survenus dans d'autres entreprises
  - Démontrer l'application de l'ERM dans des **contextes réels**
  - Fournir des exemples réels d'incidents et de fraudes d'entreprises qui auraient pu être anticipés ou atténués par une **meilleure gestion des risques**
  - Discuter de la manière dont les études de cas pourraient **concerner SCOR** et son activité
- Les cas d'étude peuvent être mis en forme et diffusés par le service communication afin d'assurer une communication engagée, pertinente et sensibilisatrice au personnel.

Exemple synthétique de cas d'étude

En 2015, un constructeur automobile a été reconnu pour avoir falsifié les tests de pollution sur 500 000 modèles diésel aux Etats-Unis. La firme avait implémenté un petit logiciel faisant apparaître des résultats inférieurs d'environ 40 fois à ceux émis en condition normale de circulation. Il s'est avéré que ce truquage n'était pas cantonné aux seuls Etats-Unis, mais à de nombreux pays européens et non-européens. Les impacts sont multiples pour le groupe allant de l'amende pour falsification de tests de qualité, aux coûts de rappel du parc automobile, au risque de réputation ou au risque d'attaques en justice des consommateurs.

Ce qui a posé problème

- La charge de la responsabilité d'avoir introduit dans le circuit de production un système de falsification, nécessitant l'approbation tacite de plusieurs responsables de sites. Jusqu'à quel niveau hiérarchique cette information était connue ? Et donc à quel niveau le processus de décision et de contrôle a-t-il pu être défaillant ?
- En plus du processus de décisions, l'approbation explicite ou tacite d'une partie des dirigeants de falsifier les tests suppose un climat permettant d'appliquer des décisions allant à l'encontre de la loi.

Ce qu'il faut retenir

- Importance de procédures d'alerte indépendantes. Dans ce cas, un ingénieur avait alerté en vain sa hiérarchie dès 2011.
- L'importance d'une culture du risque et d'éthique qui ne soit pas simplement de l'affichage. Identifier les contraintes pour exercer les bons jugements. L'exemplarité de la hiérarchie est aussi importante.
- Sans justifier aucune actions illégales, il est important de maintenir un équilibre de diversification.

Peut-il se produire le même scenario chez SCOR ?

- Si SCOR n'est pas exposé aux mêmes types de risques opérationnels, le Groupe pourrait avoir à assurer des affaires éthiquement sensibles. C'est pourquoi les guides de souscriptions imposent à tout nouveau type d'affaires des niveaux de revue impliquant les départements de gestion des risques, juridiques et selon les cas, le COMEX et le Board.

"I had to learn the importance of qualitative risk management"

Eberhard Mueller, chief risk officer of Hannover Re

Merci pour votre attention