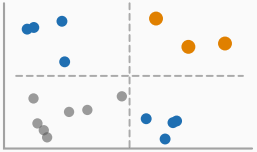
Risque opérationnel et résilience

Chapitre 6 : La communication des risques



Jaouad Madkour

Faculté d'Économie et de Gestion de Tanger · 30 août 2026

Plan du chapitre

Avant de commencer

Les destinataires du reporting

Le contenu du reporting

Les défis statistiques

Assurance et reporting externe

Synthèse

Avant de commencer

Pourquoi ce chapitre

Pourquoi ce chapitre ?

Le cycle de gestion du risque opérationnel présenté au chapitre 2 se referme par la surveillance, qui repose elle-même sur la communication : sans reporting fiable et adapté à son destinataire, l'identification (chapitre 3), l'évaluation (chapitre 4) et l'atténuation (chapitre 5) des risques restent des exercices isolés, sans effet sur les décisions. Ce chapitre étudie qui doit être informé, de quoi, et selon quels principes.

Les destinataires du reporting

Une audience à plusieurs niveaux

Six grandes catégories de destinataires

La communication du risque opérationnel s'adresse à des publics aux besoins différents : le comité des risques du conseil d'administration (supervision stratégique), le comité de direction (arbitrages opérationnels), la fonction centrale de gestion du risque opérationnel (coordination et agrégation), les responsables métiers et « champions du risque » dans les lignes d'activité (gestion quotidienne), le comité d'audit (assurance indépendante), et enfin les destinataires externes — régulateurs et public (chapitre transparence réglementaire, voir plus loin).

Le « gâteau du reporting » : trois strates

Surveiller, agir, décider

Un modèle utile distingue trois strates de reporting, empilées comme un gâteau. À la base, un reporting très détaillé sert à **surveiller** l'activité au quotidien (niveau opérationnel). Au milieu, un reporting agrégé permet d'**agir** — ajuster des contrôles, lancer des plans d'action (niveau management). Au sommet, un reporting synthétique, très sélectif, permet de **décider** des orientations stratégiques (niveau conseil d'administration). Plus on monte dans les strates, moins le volume d'information est important, mais plus son niveau d'agrégation et sa portée stratégique augmentent.

Le même événement, décliné à trois niveaux

Un incident de fraude interne isolé remonte en détail dans le reporting opérationnel du service concerné. Agrégé avec d'autres incidents similaires sur le trimestre, il alimente une tendance présentée au comité de direction. S'il révèle une faiblesse structurelle de contrôle affectant l'appétit pour le risque de l'organisation, seule sa conclusion — et non chaque occurrence — remonte au conseil d'administration.

Le contenu du reporting

Sept composantes principales

Les sept éléments d'un reporting complet

Un reporting de risque opérationnel abouti articule sept composantes : (1) le **top 10 des risques**, une liste hiérarchisée des risques les plus significatifs ; (2) la **cartographie thermique** (heatmap) et le **registre des risques**, qui visualisent probabilité et impact ; (3) les **métriques d'appétit pour le risque**, qui situent l'exposition actuelle par rapport aux limites fixées ; (4) les **indicateurs clés de risque (KRI)** et le suivi des **problèmes** (issues) ouverts ; (5) les **incidents et quasi-incidents** (near misses) ; (6) les **plans d'action** correctifs et préventifs ; et (7) les **risques émergents**, identifiés par une veille prospective (horizon scanning).

Une hiérarchisation qui force les priorités

Le modèle du « top 10 des risques » contraint l'organisation à hiérarchiser explicitement ses risques opérationnels les plus significatifs plutôt que de les présenter comme une liste plate. Associé à une cartographie thermique — probabilité en abscisse, impact en ordonnée, code couleur du vert au rouge — il offre une vue synthétique immédiatement lisible par un comité de direction ou un conseil d'administration, tandis que le registre des risques détaillé reste la référence exhaustive pour les équipes opérationnelles.

KRI, KPI et KCI : trois familles d'indicateurs

Les **indicateurs clés de risque** (KRI) mesurent l'évolution d'une exposition au risque (par exemple, le nombre de transactions en attente de validation manuelle) ; les **indicateurs clés de performance** (KPI) mesurent l'efficacité opérationnelle d'un processus ; les **indicateurs clés de contrôle** (KCI) mesurent la robustesse d'un contrôle donné (taux de complétion des vérifications obligatoires, par exemple). Un tableau de bord de risque opérationnel combine typiquement les trois familles, chacune assortie de seuils d'alerte alignés sur l'appétit pour le risque déclaré.

Étude de cas — un tableau de bord KRI en pratique

Un établissement bancaire construit un tableau de bord trimestriel de dix KRI couvrant la fraude, la continuité d'activité, la conformité et les ressources humaines, chacun assorti de trois seuils (vert, orange, rouge) calibrés sur les données historiques et l'appétit pour le risque du conseil. Le franchissement d'un seuil orange déclenche une investigation par le second niveau de contrôle ; un seuil rouge déclenche une escalade automatique au comité des risques, indépendamment du calendrier normal de reporting — illustrant que la communication du risque ne doit pas être purement périodique mais aussi événementielle.

Distinguer un problème d'un incident

Un **problème** (issue) désigne une faiblesse identifiée dans un contrôle ou un processus, avant toute matérialisation en perte — typiquement remonté par l'audit interne ou une auto-évaluation. Un **incident** est la matérialisation effective d'un risque opérationnel, avec ou sans perte financière. Un **quasi-incident** (near miss) est un événement qui aurait pu causer une perte mais qui, par chance ou grâce à un contrôle de rattrapage, ne l'a pas fait — une source d'apprentissage aussi précieuse que les pertes réelles, souvent sous-exploitée.

L’objectif zéro comme discipline de reporting

Un plan d’action correctif ou préventif n’a de valeur que s’il est suivi jusqu’à sa clôture effective. De nombreuses organisations font du nombre de plans d’action en retard un indicateur de discipline à part entière — une forme de « objectif zéro » sur les échéances non tenues — car un plan d’action qui traîne indéfiniment signale un problème de gouvernance aussi grave que le risque qu’il était censé traiter.

Horizon scanning

La veille prospective (horizon scanning) consiste à identifier systématiquement les risques émergents — nouvelles technologies, évolutions réglementaires, changements macroéconomiques ou géopolitiques — avant qu'ils ne se matérialisent en pertes. Contrairement aux composantes précédentes du reporting, qui regardent en arrière ou constatent le présent, cette composante est tournée vers l'avenir et alimente directement l'étape d'identification du cycle de gestion des risques (chapitre 3).

Les défis statistiques

L’absence de moyennes pertinentes

Des pertes à queue extrêmement épaisse

Les données de l’industrie (base ORX) illustrent un principe central du reporting du risque opérationnel : les pertes les plus importantes, supérieures à 10 millions d’euros, ne représentent que 0,4 % du nombre d’occurrences mais concentrent 66,6 % de la sévérité totale. Cette distribution extrêmement asymétrique invalide toute communication fondée sur des moyennes — une moyenne des pertes serait dominée par un petit nombre d’événements extrêmes et ne représenterait la réalité d’aucune période typique. D’où le principe : « il n’y a pas de moyennes pertinentes en risque opérationnel ».

Conséquence pour la présentation des données

Ce constat statistique a une implication directe sur la forme du reporting : privilégier les distributions, les percentiles et les événements extrêmes plutôt que les indicateurs de tendance centrale, et toujours accompagner un chiffre agrégé d’une mention de sa dispersion sous-jacente.

Trois règles pour un reporting utile

Coût-bénéfice, finalité, aide à la décision

Trois règles guident la conception d'un reporting de valeur. Premièrement, le **coût de production** de l'information doit être mis en balance avec son bénéfice pour le destinataire — un reporting exhaustif mais illisible ne vaut rien. Deuxièmement, chaque élément du reporting doit être **aligné sur une finalité** claire — à qui sert-il, et pour quelle décision ? Troisièmement, un bon reporting doit **influencer une décision** : s'il ne change jamais rien à l'action de son destinataire, il est superflu, quelle que soit sa qualité technique.

Agréger des données qualitatives

Trois méthodes d'agrégation

De nombreux risques opérationnels sont documentés qualitativement (évaluations d'auto-évaluation des risques, jugements d'experts). Trois méthodes permettent de les agréger à des fins de reporting synthétique : la **conversion en équivalent monétaire** (attribuer une valeur financière estimée à un risque qualitatif) ; la **catégorisation en paliers** (par exemple des « graphiques en chandelier » associant une échelle de couleurs à des tranches de sévérité) ; et l'approche du **pire cas plausible**, qui retient le scénario le plus défavorable raisonnablement envisageable plutôt qu'une moyenne pondérée.

Étude de cas — une cartographie thermique agrégée

Une banque combine, dans une seule cartographie thermique présentée au conseil, des risques mesurés quantitativement (pertes historiques, VaR opérationnelle) et des risques évalués qualitativement par auto-évaluation (RCSA), ces derniers étant convertis en équivalents monétaires à l'aide de barèmes internes validés par le second niveau de contrôle. Cette combinaison permet une vue unique et comparable, au prix d'une perte de granularité que le conseil accepte en échange de la lisibilité.

Assurance et reporting externe

Coordonner les trois lignes de défense

L'assurance combinée

L'assurance combinée (combined assurance) désigne la coordination des travaux des trois lignes de défense — gestion opérationnelle, fonctions de risque et de conformité, audit interne — afin d'éviter les doublons, de combler les angles morts et de fournir au conseil une vision unique et cohérente du niveau de maîtrise des risques, plutôt que trois rapports disjoints et parfois contradictoires.

Trois composantes du Pilier 3

Le Pilier 3 de Bâle impose aux banques une divulgation publique structurée en trois volets : une information **qualitative** sur la gouvernance et le cadre de gestion du risque opérationnel ; l'historique des **pertes opérationnelles** subies ; et le détail de l'**indicateur d'exploitation** (business indicator) et de ses sous-composantes, utilisé dans le calcul du capital réglementaire (chapitres 23 et 24).

Étude de cas — Credit Suisse, rapport annuel 2021

Le rapport annuel 2021 de Credit Suisse illustre les pratiques de communication du risque opérationnel au marché : détail des principales catégories de risque, description du cadre de gouvernance, quantification des pertes historiques majeures — dont les provisions liées aux affaires Archegos et Greensill — et discussion qualitative des enseignements tirés. Cet exemple montre combien la communication externe du risque opérationnel peut devenir un enjeu de crédibilité et de réputation à part entière, distinct du dispositif de gestion interne qu'elle documente.

Une extension récente : le reporting de la résilience

Le Royaume-Uni, période transitoire jusqu'en 2025

Prolongeant le cadre de résilience opérationnelle introduit au chapitre 1, les régulateurs britanniques ont imposé une période transitoire, courant jusqu'en mars 2025, durant laquelle les établissements doivent démontrer leur capacité à rester dans leurs niveaux de tolérance à l'impact pour chacun de leurs services opérationnels importants, et en rendre compte à leur superviseur. Cette exigence élargit le périmètre du reporting du risque opérationnel classique à une dimension de résilience, tournée vers la continuité du service plutôt que la seule mesure de la perte.

Synthèse

Ce qu'il faut retenir

Synthèse du chapitre

La communication du risque opérationnel s'organise en strates — surveiller, agir, décider — adaptées à des destinataires aux besoins différents, du responsable opérationnel au conseil d'administration et, in fine, au régulateur. Un reporting complet articule sept composantes, du top 10 des risques aux risques émergents, en passant par les KRI et les plans d'action. La nature à queue épaisse des pertes opérationnelles interdit tout raisonnement en moyennes et impose des méthodes spécifiques d'agrégation des données qualitatives. Enfin, l'assurance combinée entre les trois lignes de défense et le reporting externe du Pilier 3 rappellent que la communication du risque ne s'arrête pas aux portes de l'organisation : elle engage sa crédibilité vis-à-vis du marché et du régulateur.