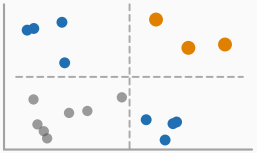
Risque opérationnel et résilience

Chapitre 4 : La mesure et l'évaluation des risques



Jaouad Madkour

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

Plan du chapitre

Avant de commencer

Les données de pertes

L'évaluation qualitative

Les modèles factoriels

La modélisation statistique

Quantifier la résilience

Synthèse

Avant de commencer

Pourquoi ce chapitre

Pourquoi ce chapitre ?

Après l'identification, ce chapitre couvre la deuxième étape du cycle : l'évaluation du risque opérationnel. Il part de la collecte des données de pertes, passe par l'évaluation qualitative (RCSA, indicateurs), puis les modèles quantitatifs (arbres de défaillance, LDA), pour finir par la modélisation du capital et la quantification de la résilience.

Les données de pertes

Le socle de toute gestion du risque opérationnel

Quatre cercles concentriques

En 2000, ING a représenté son cadre de gestion du risque opérationnel comme quatre cercles concentriques : la base de données de pertes au centre, alimentant les auto-évaluations (RCSA) au deuxième cercle, elles-mêmes surveillées par des indicateurs clés de risque (KRI) au troisième cercle, et complétées par les leçons apprises des incidents majeurs au cercle extérieur.

Les exigences réglementaires de collecte

Dix ans d'historique, seuil de 20 000 euros

Le BCBS exige, sous l'approche standardisée, un historique de dix ans de données, un seuil minimal de collecte de 20 000 euros, le rattachement de chaque perte interne aux catégories d'événements de Bâle, l'enregistrement des dates de survenue et de récupération, et une revue indépendante de l'exhaustivité et de l'exactitude des données de pertes. En pratique, de nombreux établissements retiennent des seuils plus bas (1 000 à 5 000 dollars, livres ou euros) pour ne pas perdre d'information utile à la gestion, bien que la tendance récente soit de relever ces seuils pour éviter la surcharge de déclaration.

Les événements frontières

Un événement frontière (« boundary event ») se matérialise dans une catégorie de risque différente de sa cause — par exemple une perte de crédit aggravée par une erreur d'enregistrement du collatéral. Le BCBS précise que les pertes opérationnelles liées au risque de crédit et déjà comptées dans les actifs pondérés de crédit doivent être exclues de la base de pertes opérationnelles, tandis que celles liées au risque de marché restent traitées comme risque opérationnel aux fins du calcul du capital minimal.

Les exigences réglementaires de collecte (suite)

Des champs standardisés pour une analyse fiable

Chaque incident enregistré doit suivre un jeu minimal de champs structurés — identifiant unique, lieu de survenue, catégorie de cause et de risque, contrôles ayant échoué, dates de survenue/découverte/déclaration/règlement, perte financière directe attendue, type d'impact, récupérations et perte nette. Le texte libre, utile pour la narration, ne doit jamais remplacer les champs structurés au risque de rendre l'analyse et l'agrégation automatisées impossibles.

D'autres sources pour vérifier l'exhaustivité de la collecte

Le grand livre général, les journaux d'incidents informatiques (priorités P1/P2), les provisions pour litiges, les réclamations clients et la presse négative servent de sources croisées pour évaluer si la base de données d'incidents capture bien la totalité des pertes opérationnelles matérielles — la sous-déclaration restant un défi persistant, en particulier pour les petits établissements.

L’évaluation qualitative

Risques inhérents et risques résiduels

La RCSA (auto-évaluation des risques et des contrôles) évalue la probabilité et l'impact d'un risque avant l'effet des contrôles en place (risque **inhérent**) et après (risque **résiduel**). Les échelles d'impact les plus courantes comportent quatre dimensions — financière, réglementaire, client, réputationnelle — et sont de plus en plus souvent exprimées en pourcentage du chiffre d'affaires ou des clients, pour rester comparables entre entités de tailles différentes.

Ne jamais multiplier probabilité et impact qualitatifs

Une erreur répandue consiste à multiplier une note de probabilité par une note d'impact pour produire un score numérique unique. Cette opération arithmétique sur des échelles qualitatives est trompeuse : un risque fréquent à faible impact (1×4) n'est pas équivalent à un risque rare à impact extrême (4×1), bien que le produit soit identique.

La RCSA et la carte de chaleur (suite)

Le code couleur de la carte de chaleur

La carte de chaleur (« heatmap ») combine probabilité et impact en un code couleur — vert (dans l'appétit, surveillance de routine), jaune (dans l'appétit mais en approche de la limite), ambre (au-dessus des niveaux acceptables, plan d'action requis), rouge (bien au-delà de l'appétit, action urgente requise). Ce code reflète l'appétit pour le risque de l'organisation défini au chapitre 2.

Trois familles d'indicateurs qui se recoupent

Les **KPI** (indicateurs clés de performance) mesurent l'atteinte d'objectifs opérationnels. Les **KRI** (indicateurs clés de risque) signalent l'évolution de la probabilité ou de l'impact d'un risque — par exemple une hausse du nombre de transactions par employé (risque d'erreur) ou une baisse de la satisfaction client (risque d'attrition). Les **KCI** (indicateurs clés de contrôle) mesurent l'efficacité de conception ou de fonctionnement des contrôles. Ces trois familles se recoupent largement : une défaillance de contrôle est simultanément un KPI dégradé, un KRI d'alerte et un KCI en échec.

Les modèles factoriels

Décomposer le risque en facteurs causaux

Arbres de défaillance, FAIR, Swiss Cheese, bowtie

Les modèles factoriels — analyse par arbre de défaillance (FTA), méthode FAIR, modèle du « fromage suisse », outil du « nœud papillon » (bowtie) — décomposent un scénario de risque en ses facteurs constitutifs de probabilité et d'impact, augmentant la robustesse et la transparence de l'estimation par rapport à un jugement global.

Un arbre de défaillance pour une fuite de données accidentelle

Un scénario de fuite de données par un initié peut se décomposer en cinq conditions devant toutes se réaliser : une cyberattaque ciblée par hameçonnage (P1), l'échec du pare-feu (P2), l'ouverture du courriel par un employé (P3), l'échec des contrôles détectifs de surveillance réseau (P4), et la sortie effective de l'information (P5). La probabilité conjointe de ces cinq conditions — éventuellement ajustée par des probabilités conditionnelles bayésiennes lorsque les facteurs ne sont pas indépendants — donne la probabilité du scénario complet.

Décomposer le risque en facteurs causaux (suite)

Le modèle du fromage suisse

Popularisé par le psychologue James Reason, ce modèle représente chaque couche de défense comme une tranche de fromage suisse percée de trous mouvants. Un incident grave ne survient que lorsque les trous de plusieurs couches s'alignent momentanément. La leçon pour le gestionnaire de risque : l'indépendance des défaillances de contrôles entre elles importe au moins autant que la fiabilité de chaque contrôle pris isolément.

L'analyse en nœud papillon et le « 5 pourquoi »

L'outil du nœud papillon place l'événement de risque au centre, ses causes directes et indirectes à gauche (avec les contrôles préventifs), et ses impacts directs et indirects à droite (avec les contrôles détectifs et correctifs). La technique du « 5 pourquoi » — poser la question « pourquoi cela s'est-il produit ? » au moins cinq fois de suite — permet de remonter jusqu'à la cause racine d'un incident, par exemple une mise à jour de sécurité disponible mais non déployée, elle-même due à l'absence de double compétence dans l'équipe informatique.

La modélisation statistique

L’approche par distribution des pertes (LDA)

Décomposer fréquence et sévérité

La Loss Distribution Approach (LDA) est une technique actuarielle qui modélise séparément la **fréquence** des événements de pertes (distribution discrète, le plus souvent une loi de Poisson à un seul paramètre λ) et leur **sévérité** (distribution continue, asymétrique et à queue épaisse, le plus souvent une loi log-normale), avant de les combiner par convolution — typiquement via une simulation de Monte-Carlo — pour obtenir la distribution agrégée des pertes.

Le capital économique au 99,9 centile

Le capital économique pour risque opérationnel correspond au 99,9 centile de la distribution agrégée des pertes simulées — l’établissement doit détenir un capital suffisant pour couvrir les pertes dans 999 années sur 1 000. Cette exigence exige de modéliser correctement la queue de la distribution, où les données observées sont par nature les plus rares.

Les limites de la théorie des valeurs extrêmes

La théorie des valeurs extrêmes (EVT) complète la LDA pour modéliser la queue de la distribution, mais elle repose sur une hypothèse forte : qu’un mécanisme statistique unique génère l’ensemble des pertes observées et futures. Cette hypothèse est rarement vérifiée pour un risque aussi hétérogène que

Les quatre inputs des anciens modèles AMA

Les modèles d'approches de mesure avancées (AMA), bien que remplacés par l'approche standardisée depuis 2023, continuent d'inspirer la modélisation du Pilier 2 et de l'ICAAP. Ils combinaient quatre inputs : les données de pertes internes (ILD) et externes (ELD), qui informent le passé, et les données de scénarios (SD) et les facteurs d'environnement d'affaires et de contrôle interne (BEICF), qui informent le futur prospectif.

L'ICAAP, cœur du Pilier 2

Un rapport ICAAP type couvre, entre autres, la gouvernance du processus, les méthodologies de mesure du risque, l'identification et la quantification des scénarios, et l'évaluation et la planification du capital. De nombreux établissements de taille modeste utilisent une méthode multicritère simple, réservant un capital qui excède à la fois la perte du scénario le plus sévère et celle de deux à quatre scénarios susceptibles de survenir en grappe (par exemple pandémie et cyberattaque simultanées).

Quantifier la résilience

Des services importants, pas des processus

Services opérationnels importants et tolérances d'impact

Contrairement à la gestion de continuité d'activité classique (BCM), articulée autour de chaque processus et de son délai de reprise (RTO), la résilience s'articule autour des « services opérationnels importants » (IBS) et de « tolérances d'impact » — le niveau maximal de perturbation tolérable pour un service donné, au-delà duquel un préjudice est jugé intolérable pour les clients ou pour l'intégrité du marché.

Sept étapes pour bâtir la résilience

La démarche de résilience suit sept étapes : identifier les services opérationnels importants ; fixer leurs tolérances d'impact ; cartographier les ressources et dépendances nécessaires à leur délivrance ; concevoir des scénarios sévères mais plausibles pour tester ces dépendances ; assurer, lorsque la tolérance est dépassée, un plan de communication interne et externe ; documenter et faire approuver par le conseil une auto-évaluation annuelle.

Des services importants, pas des processus (suite)

L'analyse d'impact sur l'activité (BIA) et les points de défaillance uniques

L'analyse d'impact sur l'activité (BIA) évalue les conséquences opérationnelles et financières de la perturbation d'un processus ou d'un service, et alimente directement les tolérances d'impact. Les points de défaillance uniques (SPOF) — dépendance à un employé clé détenteur d'un savoir rare, à un fournisseur informatique difficilement substituable, à un prestataire cloud unique — constituent des indicateurs clés de résilience à surveiller en priorité, et à éliminer par la redondance lorsque c'est possible.

La résilience, résultat d'une bonne gestion du risque opérationnel

Comme le rappelle le BCBS, la résilience opérationnelle n'est pas un dispositif séparé : elle est le résultat d'une gestion efficace du risque opérationnel, où l'identification, l'évaluation, l'atténuation et la surveillance des risques travaillent ensemble pour minimiser les perturbations opérationnelles et leurs effets.

Synthèse

Ce qu'il faut retenir

Synthèse du chapitre

L'évaluation du risque opérationnel part de la collecte rigoureuse des données de pertes, internes et externes, respectant les exigences réglementaires de seuil, d'historique et de catégorisation. Elle se prolonge par une évaluation qualitative (RCSA, cartes de chaleur, indicateurs KRI/KPI/KCI), des modèles factoriels qui décomposent les scénarios en facteurs de probabilité et d'impact (arbres de défaillance, FAIR, fromage suisse, nœud papillon), et une modélisation statistique (LDA, fréquence et sévérité, EVT) qui alimente le calcul du capital économique au 99,9 centile. Enfin, la quantification de la résilience — services opérationnels importants, tolérances d'impact, points de défaillance uniques — prolonge cette même logique d'évaluation vers la capacité de l'organisation à absorber et à se remettre des perturbations les plus sévères.