HIRAM FINANCE

TRANSFORMER VOS RISQUES **EN VALEUR**

Principes d'agrégation des données sur les risques et de notification des risques

BCBS 239

Défis et enjeux pour la mise en conformité

HIRAM FINANCE France
63, boulevard Haussmann , 75008 Paris
+33 1 42 66 25 25
contact@hiram-finance.com
www.hiram-finance.com

BCBS 239 : Défis et enjeux pour la mise en conformité

Dans son rapport de juin 2018[i], le BCBS fait état des travaux en cours sur la mise en conformité des établissements aux principes d'agrégation des données sur les risques et de production des reportings (BCBS 239). Il s'agit pour les banques de renforcer une capacité à disposer de données sur les risques (expositions, concentrations, etc.), fiables et agrégées au bon niveau (groupe, entité légale, business line, etc.) pour permettre un pilotage adéquat.

On retrouve là le constat, déjà établi par le BCE le mois dernier[ii], que les progrès réalisés en la matière sont bien maigres. Seules 3 banques sur les 30 soumises à l'exercice sont entièrement conformes. L'évaluation révèle que certaines institutions ont même reculé dans la mise en application de certains principes, en particulier l'exhaustivité des données et les reportings. Les autorités de tutelle s'attendent à ce que seules 13 banques soient en conformité d'ici la fin de l'année 2018, un net recul par rapport aux prévisions de 2016 – 26 banques, soit le double, étaient alors en passe de le devenir.

Les lacunes les plus sérieuses, mais également les plus nombreuses, concernent la gouvernance (principe 1) et l'architecture des données (principe 2).

Les écarts relevés (annexe, tableau 1) sont dus, en grande partie, aux difficultés qu'ont les groupes à :

- Dimensionner correctement le programme et informer la direction des obstacles rencontrés dans sa mise en œuvre.
- Surmonter les différences et contraintes au niveau des filiales (normes et standards, processus, réglementation).
- Gérer stratégiquement les projets et leurs interdépendances (l'avancement du programme dépend de la finalisation de projets connexes).
- Faire évoluer les architectures de données et architectures IT pour satisfaire les besoins opérationnels au quotidien.

Les enjeux d'un tel sujet sont multiples. Tout d'abord, il est essentiel de tirer les enseignements des difficultés et délais de mise en œuvre pour préparer les prochaines étapes. Les bonnes pratiques (tableau 2), les composants métiers, fonctionnels et techniques, doivent être soigneusement pris en compte dans les choix et le déploiement d'un dispositif efficace. À défaut, cette profusion de données de nature et de granularité différentes, parfois non réconciliées entre elles (métiers/risques/finance), lentes à produire, finit par aller à l'encontre de l'objectif initial de maîtrise des risques.

Dans un second temps, il convient de s'interroger sur la capacité des organisations à développer une stratégie d'envergure et inclusive. Les nombreuses réglementations (Bâle 3, Solvency 2, COREP/FINREP, AQR, FATCA, CRS, IFRS 9, etc.), reportings internes (capital, liquidité, etc.) parallèlement aux évolutions métiers et technologiques génèrent, certes, une explosion du volume de données, avec autant de projets distincts.

Ne serait-il possible de mener une réflexion globale en amont afin d'en tirer des synergies ? Les mêmes problématiques ne sont-elles pas rencontrées sur chaque projet ? Repenser le modèle opérationnel pour le rendre plus souple et plus agile ne permettrait-il pas de mieux anticiper les changements de demain ?

Le principe : penser autrement la conformité, non pas comme une contrainte, mais comme un levier pour impulser une véritable politique globale et établir un avantage concurrentiel par rapport aux autres institutions qui resteraient, elles, toujours dans un schéma de réglementation subie.

Il serait pertinent d'imaginer d'autres interprétations aux données, de déceler d'autres applications, y compris stratégiques, tel un cadre analytique permettant de prendre des décisions pour réaliser une répartition plus efficace du capital, une tarification plus concurrentielle des services et des produits et une meilleure gestion des coûts opérationnels.

Une réponse à ces enjeux requiert nécessairement une gestion stratégique du programme - allant au-delà du pur exercice de conformité réglementaire - voire une transformation du modèle opérationnel de la filière risques :

- La diffusion d'une nouvelle culture par la création d'une filière « data » plus intégrée qui casse les silos et intègre bien la situation (environnement, contexte, stratégie globale) et les objectifs.
- Un pilotage transverse par les processus et l'attribution de rôles et responsabilités sur les flux de bout en bout permettant d'évaluer la performance et la valeur ajoutée de chaque donnée.
- Un dispositif pérenne de gestion des données, avec des définitions et règles précises, des contrôles et la mise en place de comités permanents issus des métiers et de l'IT, approuvés par la direction.
- Une architecture des données et IT évolutive, capable d'intégrer les contraintes opérationnelles, les changements à venir et de protéger l'intégrité référentielle.

La réalisation du programme est un défi majeur pour la plupart des organisations. Par conséquent, le BCBS suggère aux organisations de prendre des actions concrètes, cohérentes avec les feuilles de route établies conjointement avec les autorités de tutelle. Cela implique une bonne gestion, tant des données que de la technologie. En l'absence d'une gestion appropriée, les problèmes seront récurrents. Fiabilisation, réactivité, automatisation, contrôle et communication sont les maîtres mots pour contribuer à la réalisation des objectifs.

Dans un contexte où les aléas ressurgissent (géopolitique, remontée des taux, inflation, etc.), susceptibles de se traduire par un regain de tension extrême sur les marchés, et compte tenu de la diversité et l'interaction des risques, les directions générales doivent pouvoir orienter leurs décisions sur la base d'informations fiables, mises à disposition rapidement. La réduction de la probabilité et l'ampleur des pertes en dépendent.

Annexe - Tableau 1 : Principaux écarts de conformité observés par le comité de Bâle :

Gouvernance et infrastructure (principes 1 et 2)	P1. Gouvernance	— Absence de politique et de cadre cohérents pour permettre à la direction générale d'évaluer la mise en œuvre du programme. — Attention trop forte portée sur la résolution de problèmes ponctuels, au détriment de l'amélioration globale de la gouvernance. — Inadéquation des pratiques de gestion de projet : des projets sont souvent mal dimensionnés, avec par conséquent des feuilles de route et retro planning inadaptés ; un manque de transparence sur les progrès de mise en œuvre et l'évolution des coûts ; un manque d'expertise technique. — Manque de cohérence de la gouvernance entre les diverses entités.
	P2. Architecture des données et infrastructure IT	— Mauvaise gestion des incidents et des anomalies, en particulier la remontée des alertes. — Inadéquation des processus et des contrôles pour permettre la mise à jour des données à la suite d'évènements. — Incapacité à intégrer les taxonomies et l'architecture de certaines filiales étrangères.
Capacité d'agrégation des données sur les risques (principes 3 à 6)	P3. Exactitude et Intégrité	— Présence notable et excessive de processus manuels d'agrégation, sans documentation adéquate. — Manque de progrès, en raison de la dépendance à l'égard des solutions IT non encore déployées. — Manque de standardisation des données de référence par les fonctions Risques et Finance. — Contrôles de qualité insuffisants (incapacité à cartographier et intégrer les normes de qualité des données, à établir les règles de qualité.
	P4. Exhaustivité	— Présence notable et excessive de processus manuels d'agrégation, sans documentation adéquate. — Manque de progrès, en raison de la dépendance à l'égard des évolutions des systèmes d'information en cours et des solutions non encore déployées. — Insuffisance des contrôles de qualité (incapacité à cartographier et intégrer les normes de qualité, les règles sont insuffisamment établies).
	P5. Actualité	— Incapacité à recueillir et agréger les données des filiales étrangères en temps opportun.
	P6. Adaptabilité	— Évolution et l'adaptation des méthodes et procédures d'agrégation ne sont pas suffisamment maîtrisées, en réponse aux changements de business models et du cadre réglementaire. — Pas de rapprochement de certains indicateurs clés entre les fonctions Risques et Finance
Pratiques de notification des risques (principes 7 à 11)	P7. Exactitude	— Inexactitudes dans certains rapports : des données ne sont pas mises à jour à cause de processus d'agrégation trop complexes et délais de validation trop importants. — Les rapports de risque ne sont pas validés en raison de contrôles insuffisants et de règles ou procédures de validation inadéquates. — Processus de signalements et de correction des erreurs non intégrés au sein des processus métier.
	P8. Représentativité	— Manque de granularité des données car les différentes catégories et sous-catégories de risque (risque de crédit général et risque de contrepartie) ne sont pas représentées. — Manque de prévisions prospectives et de simulations de crise, ce qui ne permet pas d'identifier les signaux faibles. — Contraintes légales qui empêchent les banques de collecter des données auprès des filiales étrangères.
	P9. Clarté et utilité	— Rapports statiques et ne sont pas complétés par des rapports de type tableau de bord plus dynamiques.
	P10. Fréquence	— Une confiance trop grande dans les processus manuels pour produire les rapports, représentant un obstacle à une production rapide des rapports ponctuels ou en situations de crise.

Annexe - Tableau 2 : Bonnes pratiques recensées par le comité de Bâle :

Gouvernance	— Intégrer la gouvernance des données dans le cadre global de gestion des risques. — Définir les exigences en matière de données à l'échelle de la banque. — Élaborer et faire appliquer les règles et bonnes pratiques en matière de gestion des données (rôles et responsabilités, contrôle, qualité, moyens, suivi des actions), adaptées au contexte des risques. — Communiquer à intervalles réguliers les initiatives et les progrès de mise en œuvre au conseil d'administration et à l'ensemble de la banque.
Infrastructure	— Allouer les ressources adéquates pour intégrer les bases de données des différentes entités juridiques, filiales et succursales. — Identifier les technologies et processus redondants ou inefficaces. — Consolider les approches et structures de classification des données ainsi que les taxonomies. — Élaborer un dictionnaire et un référentiel unique pour chaque type de risque. Prendre des mesures efficaces pour gérer les informations clients en s'appuyant sur les normes en vigueur (p. ex. le LEI). — Lancer des projets visant à évaluer la qualité des données et mettre en place des actions correctives sur l'ensemble du périmètre de la banque — Mettre en place des plans efficaces de continuité des opérations et tester régulièrement les systèmes de sauvegarde.
Capacité d'agrégation des données sur les risques	— Dégager des capacités techniques pour agréger automatiquement les données des filiales étrangères. Par exemple, en utilisant un modèle de métadonnées développé au niveau du groupe, une banque a pu intégrer et centraliser les données de base pour tous les types de risques. — Établir des taxonomies dans l'ensemble du groupe. — Réaliser des contrôles de qualité adéquats et des suivis réguliers. — Formaliser les processus de rapprochement des données.
Pratiques de notification des risques	— Des rapports précis de gestion des risques et en temps opportun, durant les périodes normales et en temps de crise, doivent être produits et rapidement distribués en interne (y compris le conseil d'administration et le comité exécutif) et aux autorités de tutelle. — Les reportings doivent intégrer l'analyse des différents types de risques et être présentés sous des tableaux de bord dotés d'une interface simple et conviviale. — Les rapports doivent (i) porter sur l'analyse de l'évolution des tendances de risque et des risques potentiels; (ii) présenter des analyses de scénario et stress tests ; et (iii) contenir des mesures de gestion des risques. — La filière Risques maintient des procédures pour produire des rapports précis, dans la durée. — Les rapports sont conçus automatiquement, avec des données fiables, provenant d'une source unique ; les rapports manuels qui sont en cours d'automatisation doivent contenir des contrôles appropriés pour garantir l'exactitude des données. — Les rapports couvrent tous les types de risques (crédit, marché, opérationnel, liquidité, réputation, pays) et montrent les concentrations dans les secteurs et zones géographiques clés. — Les rapports sur les risques sont produits à la fréquence appropriée et adaptés au conseil d'administration et au comité exécutif ; en particulier, les éléments spécifiques adressés au management doivent être mis en évidence. Les rapports sont également suffisamment détaillés en termes de contenu, ce qui permet au conseil et / ou à la haute direction de prendre des décisions éclairées. — Le conseil d'administration et le comité exécutif prennent des mesures pour déterminer le périmètre des données nécessaires pour faire face à une crise, en ayant pris soin de préparer des modèles à l'avance. — Un canal de distribution, avec différents niveaux d'accès, doit servir sert de point d'entrée unique pour tous les rapports pertinents. Grâce au cryptage des fichiers et au contrôle par le système d'information, la confidentialité des rapports sur les risques est assurée de manière appropriée.

Annexe - Tableau 3 : Les 11 principes du BCBS à destination des banques [iii]

Gouvernance et infrastructure (principes 1 et 2)	P1. Gouvernance	Les capacités d'agrégation des données sur les risques d'une banque et ses pratiques de reporting des risques doivent faire l'objet d'un dispositif de gouvernance solide.
	P2. Architecture des données et infrastructure IT	L'architecture des données et l'infrastructure informatique sont conçues, mises en place et gérées pour renforcer les capacités d'agrégation des données sur les et les pratiques de reporting des risques en situation normale et en période de crise.
Capacité d'agrégation des données sur les risques (principes 3 à 6)	P3. Exactitude et Intégrité	Les données sur les risques sont exactes et fiables pour satisfaire aux exigences d'exactitude applicables aux reportings, en temps normal comme en période de crise (l'agrégation des données doit, pour l'essentiel, être automatisée).
	P4. Exhaustivité	Les données sur les risques doivent être agrégées et consultables par ligne de métier, entité juridique, type d'actif, secteur, région et autre, pour un risque donné, afin de permettre l'identification et le reporting des expositions, des concentrations de risques et des risques émergents.
	P5. Actualité	Les données sur les risques doivent être rapidement produites, agrégées et mises à jour, dans les délais appropriés au risque (en fonction de sa nature, volatilité et importance pour le groupe).
	P6. Adaptabilité	Les données sur les risques agrégées permettent de faire face à toutes sortes de demandes de reporting ponctuels, notamment émises en période de tensions ou de crise, liées à une modification des besoins internes et provenant des autorités de contrôle.
Pratiques de notification des risques (principes 7 à 11)	P7. Exactitude	Les reportings doivent présenter de façon précise et exacte des données Risques agrégées et donner une représentation fidèle des risques encourus par l'établissement (ils doivent faire l'objet de rapprochements et validation).
	P8. Représentativité	Les reportings doivent couvrir toutes les grandes familles de risques auxquelles l'organisation est exposée, le degré d'approfondissement de ces reportings et les questions qu'ils abordent étant fonction de la taille et de la complexité des opérations menées par la banque, de son profil de Risque et des exigences des destinataires.
	P9. Clarté et utilité	Les reportings doivent être clairs, concis, faciles à comprendre tout en étant suffisamment complets pour permettre aux destinataires de prendre des décisions en toute connaissance de cause (les informations dont ils font état doivent être pertinentes et adaptées aux besoins des destinataires).
	P10. Fréquence	La fréquence de production et de distribution des reportings Risques est définie par le conseil d'administration et à la direction générale, en fonction des besoins des destinataires, de la nature des Risques notifiés et de la vitesse à laquelle le Risque peut changer et cette fréquence doit augmenter en période de tensions ou de crise.
	P11. Distribution	Les reporting sont distribués aux parties concernées en veillant à préserver leur caractère confidentiel.

Références

[i] https://www.bis.org/bcbs/publ/d443.htm

[ii] Report on the Thematic Review on effective risk data aggregation and risk reporting, May 2018 - https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.BCBS_239_report_201805.pdf

[iii] Principes aux fins de l'agrégation des données sur les risques et de la notification des risques, janvier 2013 – https://www.bis.org/publ/bcbs239_fr.pdf