ALTEAM
EXPERT DES PROGICIELS DE LA FINANCE

BIA
CONSULTING
BUSINESS INTEGRITY ANALYSIS

BCBS 239

Basel committee on banking supervision

Table des matières

1. Introduction 3
2. Objectifs 3
3. Champs d'application 3
4. Description de la réglementation BCBS 239 4
   - Les 11 principes concernant les établissements bancaires 4
   - Les 3 principes concernant les autorités de contrôle 5
4. Impacts 6
5. Lexique 7
6. Source 7

1. Introduction

La réglementation **BCBS (Basel Committee on Banking Supervision) 239** a été publiée par le Comité de Bâle en janvier 2013 (dernière version). Elle vient renforcer le Pilier 2 des réglementations Bâle 2 / Bâle 3 qui a pour objet la surveillance par les autorités prudentielles et par les banques elles-mêmes, des différents risques. Un certain nombre de principes présentés ci-après ont été élaborés dans cette optique.

BCBS 239 porte sur l'agrégation des données risques et leurs reporting. L'objectif est principalement d'améliorer la qualité des données afin de pouvoir générer des reporting adéquats ; et de permettre une meilleure analyse du risque que ce soit au sein des banques ou au niveau des régulateurs.

Elle fait suite à la crise financière de 2007/2008 qui a mis en exergue certaines problématiques des banques dans la gestion de leurs données Risques. La multiplicité et l'hétérogénéité des systèmes d'information bancaires peuvent, en effet, poser problèmes pour la mise en œuvre de reporting fiables et pour le pilotage des risques judicieux.

Au niveau européen, elle est appliquée par la Banque Centrale Européenne, qui délègue une partie des activités aux superviseurs nationaux.

Remarque : Le Comité de Bâle définit le terme « agrégation des données risques » comme désignant la définition, la collecte et le traitement des données selon les exigences de reporting risques de la Banque. L'objectif est de lui permettre d'évaluer son rendement en fonction de sa prise de risque. Cela inclut le tri, la fusion et la décomposition des jeux de données.
-> les données doivent être modulables de manière à pouvoir être interprétées et évaluées en fonction des différents axes d'analyses choisis.

2. Objectifs

L'application des principes issus des recommandations BCBS 239 permettra d'apporter des améliorations fondamentales au sein des banques, en termes de gestion et notamment :

- Améliorer l'infrastructure afin de favoriser le reporting des informations clés, utilisé par les différentes Directions pour identifier, surveiller et gérer les risques
- Améliorer les processus décisionnels dans l'ensemble de l'organisation bancaire
- Améliorer la gestion de l'information entre les entités juridiques, tout en facilitant une vision consolidée des risques d'exposition
- Réduire la probabilité et la gravité des pertes liées à des manquements dans la gestion des risques
- Améliorer le délai de disponibilité des informations pour améliorer le délai de prise de décision
- Améliorer la qualité de planification stratégique de l'organisation et la gestion du risque lié à de nouveaux produits et services

3. Champs d'application

Ces recommandations concernent les établissements bancaires d'importance systémique, les **SIB (Systemically Important Banks)**. Elles s'appliquent au niveau de chaque filiale/entité et au niveau plus global du groupe. Les superviseurs nationaux ont la possibilité d'élargir ce périmètre d'application à d'autres établissements bancaires, le cas échéant.

Le FSB (Financial Stability Board) définit si un établissement bancaire entre dans le périmètre cible de BCBS 239. Ces établissements bancaires sont dénommés **G-SIB (Global Systemically Important Banks).** Les G-SIB identifiés en 2011 ou 2012, doivent s'y conformer **depuis janvier 2016**. Par la suite, un établissement lorsqu'il est identifié dispose de **3 ans pour se mettre en conformité**.

Les superviseurs nationaux pourront désigner les établissements **D-SIB (Domestic Systemically Important Banks)**, qui auront également **3 années pour se mettre en conformité**.

30 G-SIBs identifiées par le FSB (Novembre 2017) dont BNP Paribas, Société Générale et Groupe Crédit Agricole.

La réglementation BCBS 239 vise en particulier les principaux domaines de risques, à savoir :

- Risque de crédit,
- Risque de marché,
- Risque de liquidité,
- Risque opérationnel.

4. Description de la réglementation BCBS 239

La norme **BCBS 239 pose 14 principes**. 11 concernent les établissements bancaires. 3 concernent les autorités de contrôle qui devront surveiller ces établissements. Elle est intitulée « Principles for effective Risk Data Aggregation and risk Reporting (RDAR) ».

Les 11 principes concernant les établissements bancaires

Ces 11 principes sont structurés en trois thématiques :

1. Gouvernance globale et infrastructure

La banque devrait avoir un système de gouvernance robuste, ainsi qu'une architecture des données risques et une infrastructure appropriées. Le remplissage de ces conditions est nécessaire au respect des autres principes. En particulier, **le Conseil d'Administration** de la banque devrait veiller à ce que les directions mettent en œuvre les principes d'agrégation des données risques et les reporting relatifs à ces données ; en respectant le délai déterminé par les autorités de contrôle. (cf Tableau)

2. Capacités d'agrégations des données risques

La banque devrait développer et maintenir de fortes capacités d'agrégation des données risques afin de s'assurer que les reporting produits sur la base de ces données reflètent effectivement le risque encouru, de manière fiable. L'application des différents principes ne doit pas s'effectuer au détriment les uns des autres. Les capacités d'agrégation des données risques doivent satisfaire tous les principes énoncés à ce sujet (cf Tableau).

3. Pratiques de reporting des risques

Des donnés complètes, précises et à jour sont une condition nécessaire à une gestion des risques efficace. Néanmoins, les données seules ne suffisent pas à garantir des bonnes prises de décision, en termes de risque, par le Conseil d'Administration et les hautes directions. Pour gérer le risque de manière efficace, les bonnes informations doivent être présentées au bon moment et aux personnes adéquates. Les reporting générés devraient donc être exacts, clairs et complets. Ils devraient fournir un contenu approprié aux décideurs adéquats et dans un délai permettant une réponse pertinente. (cf Tableau)

Gouvernance globale et Infrastructure	
Principe 1 : Gouvernance	Les capacités d'agrégation des données risques et les pratiques de reporting risques devraient être intégrées aux règles de gouvernance, en accord avec les autres principes bâlois.

Principe 2 : Architecture des données et infrastructure	L'architecture et l'infrastructure des SI devraient permettre de gérer les données et les reporting risques que ce soit en temps normal ou en période de stress ou de crise.
Capacités d'agrégation des données risques	
Principe 3 : Exactitude et intégrité	Les données devraient être précises et fiables afin de pouvoir générer des reporting de qualité que ce soit en temps normal ou en période de stress/crise. Les données devraient être agrégées de manière largement automatisée afin de minimiser les erreurs.
Principe 4 : Exhaustivité	Les données devraient être agrégées au niveau groupe. Elles devraient être disponibles par secteur d'activité, par entité juridique, par type d'actif ; et tout autre axe permettant d'évaluer le risque.
Principe 5 : Rapidité	Les données devraient pouvoir être fournies de manière rapide, tout en étant actualisées, fiables et exhaustives. Le délai devra dépendre du type de risque évalué, notamment en fonction de la volatilité et des impacts globaux de celui-ci ; ainsi que des exigences de reporting propres à l'établissement que ce soit en temps normal ou en période de stress/crise.
Principe 6 : Adaptabilité	Les données fournies devraient pouvoir être agrégées en fonction du besoin du reporting, en incluant les exigences liées aux périodes de stress/crise, celles liées aux mouvances internes et celles liées aux demandes des autorités de supervision.
Pratiques de reporting des risques	
Principe 7 : Exactitude	Les reporting de gestion des risques devraient transmettre avec exactitude et précision, les données risques agrégées ; et refléter précisément le risque. Ces reporting doivent être réconciliés et validés.
Principe 8 : Complétude	Les reporting de gestion des risques devraient couvrir tous les domaines de risque de l'organisation. Le périmètre doit être établi en tenant compte de la complexité des opérations, du profil de risque de l'entité, ainsi que des exigences des destinataires.
Principe 9 : Clarté et utilité	Les reporting de gestion des risques devraient permettre de communiquer l'information de manière claire et concise. Les rapports devraient être facilement compréhensibles mais suffisamment exhaustifs pour permettre une prise de décision avisée. Les rapports devraient contenir les informations utiles adaptées aux besoins des destinataires.
Principe 10 : Fréquence	Le conseil d'administration et la direction générale notamment devraient définir la fréquence de production et de distribution des reporting de gestion des risques. Ces fréquences devront dépendre des besoins des destinataires, de la nature du risque et de la rapidité avec laquelle le risque peut changer, ainsi que de l'importance de la contribution des reporting pour évaluer les risques et pour une prise de décision efficace. La fréquence des reporting devrait augmenter en période de stress/crise.
Principe 11 : Distribution	Les reporting de gestion des risques devraient être transmis aux acteurs adéquats tout en préservant la confidentialité des données, le cas échéant.

Les 3 principes concernant les autorités de contrôle

Ces 3 principes sont regroupés sous la thématique :

- **Supervision, outils et coopération**

Les superviseurs auront un rôle important à jouer dans la surveillance, l'incitation à la mise en œuvre et au respect continu des différents Principes par les établissements financiers. Ils devraient également s'assurer,

au travers des différentes expériences menées par les différents établissements, que ces Principes atteignent bien leurs objectifs et évaluer si des améliorations s'avèrent nécessaires.

Supervision, outils et coopération	
Principe 12 : Surveillance	Les autorités de contrôle devraient revoir et évaluer périodiquement la conformité des établissements bancaires aux 11 principes précédents.
Principe 13 : Actions correctives et mesures prudentielles	Les autorités de contrôle devraient avoir la possibilité d'exiger aux établissements financiers des mesures correctives efficaces si des lacunes sont observées dans leur gestion des données ou des reporting risques. Les superviseurs devraient pour ce faire, utiliser une gamme d'outils, y compris ceux du Pilier 2.
Principe 14 : Coopération entre les autorités prudentielles	Les autorités de contrôle devraient coopérer entre elles, lorsqu'il s'agit notamment de mettre en place des mesures correctives, ainsi que dans le cadre de la surveillance ou de la modification des Principes.

4. Impacts

Cette réglementation présente des impacts forts sur les SI que ce soit en terme d'infrastructure, d'architecture et en termede gestion des processus.

Les banques vont devoir (et ont déjà dû) s'adapter et mettre en œuvre des SI centralisés, en mutualisant les données et en permettant d'avoir des références uniques.

Le SI devient un acteur d'aide de prise à la décision, dans le cadre de la gestion des risques notamment et doit permettre de répondre aux exigences réglementaires.

5. Lexique

BCBS 239 (Basel Committee on Banking Supervision)
SIB (Systemically Important Banks)
G-SIB (Global Systemically Important Banks)
D-SIB (Domestic Systemically Important Banks)
RDAR (Risk Data Aggregation and Reporting)

6. Source

https://www.bis.org/publ/bcbs239.pdf

http://financialmarketsjournal.co.za/bcbs-239-risk-data-aggregation-and-reporting/

http://www.decideo.fr/BCBS-239-ou-savoir-revenir-aux-bases-de-la-gestion-des-donnees-de-risques-pour-eviter-une-nouvelle-crise-financiere_a7173.html

http://www.fsb.org/wp-content/uploads/r_121031ac.pdf?page_moved=1