

# Risque opérationnel : les enjeux réglementaires pour les banques

1. **Aspects quantitatifs : évolutions attendues du cadre réglementaire avec Bâle 3**
2. **Aspects qualitatifs : place des risques opérationnels dans la gestion des risques et la gouvernance**

# 1. Aspects quantitatifs (1/4)

## Deux principales lacunes dans le cadre existant

- 1 Exigences de fonds propres insuffisantes pour couvrir les pertes de certaines banques imputables aux risques opérationnels
- 2 La nature des pertes liées à des comportements répréhensibles ou à des systèmes et contrôles inappropriés

➔ Besoin de changer de mesure

➔ Difficulté de recourir aux modèles internes



**Une seule approche standard de mesure du risque opérationnel**

# 1. Aspects quantitatifs (2/4)

Nouvelle **approche standard** remplaçant toutes les approches existantes avec :

- une mesure du revenu de la banque (*Business Indicator Component*, BIC, fondé sur les revenus des activités de crédit, de services et d'investissement)
- une mesure des pertes historiques (*Internal Loss Multiplier*, ILM)

Charge en capital calculée comme :  $ORC = BIC \cdot ILM$

Calibrage :

Indicateur d'activité (BIC)

Buckets	<u>Accord final</u>
1 : 0 → 1 Mds €	12%
2 : 1 → 30 Mds €	15%
3 : 30 → ∞	18%

Facteur « pertes » (*Loss component*, LC, au sein de l'ILM).

Données	<u>Accord final</u>
<b>Pertes sur les 10 dernières années</b>	15 fois les pertes historiques moyennes

Le facteur « pertes » est (pour les banques en *bucket* 1) ou peut être (sur décision de supervision, pour les autres banques) « neutralisé » en étant valorisé à 1

➔ La charge en capital pourrait ainsi être calculée uniquement sur le facteur « revenus » (BIC)

# 1. Aspects quantitatifs (3/4)

## Enjeu de la transposition BIII : quelle mise en œuvre européenne ?

- Il appartiendra au législateur européen (et à l'ABE si elle en reçoit mandat) de préciser :
  - La mise en œuvre des **options** prévues par le Comité de Bâle (ILM = 1, exclusion de certaines pertes, augmentation du seuil de collecte des pertes) : harmonisation au niveau 1 ou option laissée aux superviseurs ou aux États membres ?
  - La **fréquence** et les **modalités de reporting** au superviseur
  - Les conditions dans lesquelles les établissements devront intégrer les historiques de données liées à des acquisitions ou pourront être autorisés à exclure des historiques de données de pertes celles liées à des activités cédées
- ➔ Les autorités ont engagé des **analyses de l'incidence du passage du régime actuel à Bâle 3**. Ces résultats, et notamment le futur rapport de l'ABE répondant au *Call for Advice* de la Commission Européenne sur Bâle III, permettront d'orienter les décisions lors de la transposition dans le cadre prudentiel européen.

# 1. Aspects quantitatifs (4/4)

## Quelles conséquences ?

- ❑ **La fin des modèles internes (AMA) et des autres approches** « standards » actuelles, au profit d'une **formule standard commune plus simple et renforcée**.
- ❑ Une plus grande **comparabilité** entre les profils de risque opérationnel des différents établissements et une plus grande **transparence**, y compris pour les analystes externes (*disclosure*).
- ❑ **ICAAP** (non couvert par le standard BIII) : quelle adaptation pour les établissements, notamment avec la fin des AMA ?
- ❑ Avant CRR3, **les banques disposant d'un AMA doivent s'assurer qu'elles respectent les dispositions du RD 2018/959** (« RTS AMA ») qui entreront en application, pour la plupart, en juillet 2019.

## 2. Aspects qualitatifs (1/4)

### La gestion qualitative du risque : un enjeu aussi important

- ❑ La mise en œuvre des nouvelles dispositions quantitatives doit être **accompagnée de mesures d'ordre organisationnel**.
- ❑ En effet, le risque opérationnel est au **cœur des dispositifs de gestion de risques** des établissements et les efforts doivent être poursuivis :
  - en respectant les « **3 lignes de défense** » et leur gouvernance (implication des dirigeants et de l'organe de surveillance, indépendance du contrôle, audit...),
  - en améliorant la **mesure et l'identification des risques**, et la **réactivité** aux problèmes (qualité des données, tests & indicateurs « clés », information centralisée...),
  - en ayant une **approche globale des risques** (définition d'une appétence au risque notamment).
- ❑ D'autant plus important que des **faiblesses persistent alors que certains risques croissent** :
  - surveillance imparfaite du **périmètre d'activité** (entités étrangères, lignes de métier périphériques...), dans un contexte de nouvelle concurrence par les FinTech
  - nécessité d'une adéquation des **moyens affectés au contrôle interne**
  - prise en compte imparfaite de certains risques (**risque juridique** ou **risque informatique** en particulier), dans un contexte où ils ont pris une ampleur et une complexité nouvelles.

## 2. Aspects qualitatifs (2/4)

### Les dispositions existantes appelées à évoluer

- ❑ Le standard Bâle III couvre peu les problématiques de **gouvernance** et d'**organisation de la gestion du risque opérationnel**, mais de nombreuses dispositions existent déjà en la matière :

	Dispositions contraignantes	Autres références (sélection)
Au niveau bâlois		<ul style="list-style-type: none"> <li>- <i>Principles for the Sound Management of Operational Risk (PSMOR)</i> – juin 2011</li> <li>- <i>Supervisory Guidelines for the Advanced Measurement Approaches</i> – juin 2011</li> <li>- <i>Principes aux fins de l'agrégation des données sur les risques et de la notification des risques ("BCBS 239")</i> – janvier 2013</li> </ul>
Au niveau européen	<ul style="list-style-type: none"> <li>- <b>CRD</b> : art. 85 (Plans de continuité d'activité)</li> <li>- <b>CRR</b> :               <ul style="list-style-type: none"> <li>=&gt; Information de la Direction Générale (cf. art.320 c. et 321 c.)</li> <li>=&gt; Système d'évaluation du risque opérationnel intégré aux processus de gestion des risques de l'établissement (cf. art. 320 b. et 321 a.)</li> <li>=&gt; Indépendance de la fonction de gestion du risque opérationnel (cf. art. 321 b.)</li> <li>=&gt; Assurance du risque et autres mécanismes de transfert des risques (cf. art. 323)</li> </ul> </li> <li>- <b>Règlement délégué (UE) 2018/959</b> précisant la méthode d'évaluation en vertu de laquelle les autorités compétentes autorisent les établissements à utiliser des approches par mesure avancée pour le risque opérationnel (surnommé "RTS AMA") (cf. art. 1 à 24 – mars 2018)</li> </ul>	<ul style="list-style-type: none"> <li><b>Orientations de l'ABE sur l'externalisation</b> – février 2019</li> <li><b>Orientations de l'ABE sur la gouvernance interne</b> - septembre 2017</li> </ul>
Au niveau national	<b>Arrêté relatif au contrôle interne</b> – novembre 2014	<b>Document de réflexion de l'ACPR sur le risque informatique</b> - janvier 2019 (2e version post consultation publique)

- ❑ **CRD V** : référence supplémentaire au risque opérationnel lié à l'externalisation (art. 85)

## 2. Aspects qualitatifs (3/4)

### Une problématique particulière : le risque cyber

#### □ Vers une **harmonisation du cadre aujourd'hui fragmenté** :

- FSB : rapport *Stocktake of publicly released Cybersecurity regulatory and supervisory practices* (octobre 2017) et **Cyber Lexicon** (novembre 2018)
- G7 : différents lots de **Fundamental Elements** relatifs à la cybersécurité publiés depuis 2017, (ex. concernant le cyber-risque de tiers et les tests d'intrusion en octobre 2018) et réalisation d'un **exercice de simulation de crise dans le cadre de la présidence française** en 2019
- BCBS : *Cyber-résilience : range of practices* (décembre 2018)
- Union Européenne :
  - ✓ **FinTech Action Plan de la Commission Européenne** (mars 2018) invitant notamment les AES à faire l'inventaire des pratiques nationales de surveillance en matière de sécurité informatique et à évaluer les coûts et avantages de l'élaboration d'un cadre cohérent de test de la cyber-résilience destiné aux participants et infrastructures majeurs des marchés
  - ✓ **Orientations SREP de l'ABE sur l'évaluation du risque informatique dans la procédure SREP** (septembre 2017), et nouvelles orientations ABE relatives au risque informatique à venir (fin de la consultation publique mi-mars 2019)
  - ✓ **Méthodologie TIBER-EU de la BCE** sur les tests d'intrusion fondés sur des procédures d'« intelligence » (mai 2018)



# MERCI DE VOTRE ATTENTION

---

