Risques opérationnels : les enjeux réglementaires

LA GESTION DES RISQUES OPÉRATIONNELS
À UN TOURNANT DE SON ÉVOLUTION

Paris, le 25 septembre 2018 Frédéric VISNOVSKY Secrétaire général adjoint

Risques opérationnels : les enjeux réglementaires

1. **Les évolutions attendues du cadre réglementaire avec Bâle 3**

2. **La place des risques opérationnels dans la gestion des risques et la gouvernance**

3. **Un enjeu particulier : la gestion du risque informatique**

1. Les évolutions attendues du cadre réglementaire avec Bâle 3 (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

→ Besoin de changer de mesure

2. La nature des pertes liées à des comportements répréhensibles ou à des systèmes et contrôles inappropriés

→ Difficulté de recourir aux modèles internes

Une seule approche standard de mesure du risque opérationnel

1. Les évolutions attendues du cadre réglementaire avec Bâle 3 (2/4)

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

- Une mesure du revenu de la banque (*Business Indicator Compo*nent, BIC)
- Une mesure des pertes historiques (*Internal Loss Multiplier*, ILM)

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

Calibrage :

Indicateur d'activité (*Business Indicator Component*, BIC)

Buckets	Accord final
1 : 0 ➔ 1 Mds €	12%
2 : 1 ➔ 30 Mds €	15%
3 : 30 ➔ ∞	18%

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

Données	Accord final
Pertes sur les 10 dernières années	15 fois les pertes historiques moyennes

Le facteur « pertes » est (pour les banques en *bucket* 1) ou peut être (par discrétion nationale, pour les autres banques) « neutralisé » en étant valorisé à 1

➡ La charge en capital pourrait ainsi être calculée sur la seule base du facteur « revenus » (BIC)

1. Les évolutions attendues du cadre réglementaire avec Bâle 3 (3/4)

Quelle mise en œuvre au niveau européen ?

- **Il appartiendra au législateur européen de préciser :**
  - Comment les options nationales prévues par le Comité de Bâle (ILM = 1 ou exclusion de certaines pertes) doivent être mise en œuvre (harmonisation par le niveau 1, option laissée aux superviseurs ou aux États membres)
  - À quel niveau (consolidé, sous-consolidé, individuel) le calcul du ratio doit être effectué et sur quel périmètre d'établissements (le standard s'appliquant par défaut aux « *internationally active banks* »)
- **Il appartiendra au législateur ou à l'autorité bancaire européenne de préciser :**
  - 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

1. Les évolutions attendues du cadre réglementaire avec Bâle 3 (4/4)

Quelles conséquences ?

- **La fin des modèles internes** (AMA) et des autres approches « standards » actuelles, au profit d'une **formule commune plus simple et plus sensible aux risques**.
- 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*).
- Un **renforcement des fonds propres**, donc de la stabilité financière.
- Des **règles de gestion** de la collecte et du traitement des données relatives aux pertes qui visent à **garantir la qualité de l'information**.

➔ Le Comité de Bâle et l'Autorité bancaire européenne (à la demande de la Commission) ont engagé des **analyses de l'incidence du passage du régime actuel à Bâle 3**, ces travaux s'échelonnant jusqu'à 2022 et supposent la **participation des établissements** (QIS, Collecte *Call for Advice* Bâle 3).

➔ La mise en œuvre standard réglementaire (quantitatif) doit être accompagnée des **mesures d'ordre organisationnel** parfois déjà existantes et à renforcer.

2. La place des risques opérationnels dans la gestion des risques et la gouvernance (1/4)

Les principales dispositions qualitatives du cadre européen

- Le standard Bâle III ne couvre pas les problématiques de **gouvernance** et d'**organisation de la gestion du risque opérationnel**, dont il existe des références dans le cadre européen actuel (article 85 de CRD, et articles 320 à 323 de CRR) :
  - **Information de la Direction Générale** (cf. art. 320 c. et 321 c. CRR)
  - **Système d'évaluation du risque opérationnel intégré aux processus de gestion des risques de l'établissement** (cf. art. 320 b. et 321 a. CRR)
  - **Indépendance de la fonction de gestion du risque opérationnel** (cf. art. 321 b. CRR)
  - **Assurance du risque et autres mécanismes de transfert des risques** (cf. art. 323 CRR)
  - **Plans de continuité d'activité** (art. 85 CRD)

- A court terme, dans **CRD V**, une **référence supplémentaire au risque d'externalisation** sera intégrée (art. 85), afin de lui donner une importance plus forte dans la gestion du risque opérationnel.

➔ Lors de la mise en œuvre du standard Bâle III au niveau européen, il s'agira de **maintenir ces dispositions**, voire de les renforcer.

La place des risques opérationnels dans la gestion des risques et la gouvernance (2/4)

Les références existantes qui sont pertinentes

	Références	Objets
Au niveau bâlois	*Principles for the Sound Management of Operational Risk (PSMOR) – juin 2011*	Onze principes "qualitatifs" de gestion et gouvernance du risque opérationnel
	Supervisory Guidelines for the Advanced Measurement Approaches – juin 2011	Applicable aux modèles internes, mais contenant des éléments organisationnels qui demeurent pertinents pour la gestion du risque
	Principes aux fins de l'agrégation des données sur les risques et de la notification des risques ("BCBS 239") – janvier 2013	Ensemble de principes qui visent à renforcer la capacité des banques à agréger les données relatives aux risques et à améliorer les pratiques de notification des risques à l'intérieur des établissements
Au niveau européen	Orientations du CEBS sur l'externalisation – décembre 2006	Douze orientations relatives à la gestion de l'externalisation, en cours de mise à jour par l'EBA
	Règlement délégué (UE) 2018/959 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") – mars 2018	Applicable aux modèles internes, contenant des éléments organisationnels qui demeurent pertinents pour la gestion du risque
Au niveau national	Arrêté relatif au contrôle interne – novembre 2014	Texte de référence pour le contrôle interne, avec des dispositions particulières relatives au risque opérationnel et à l'externalisation

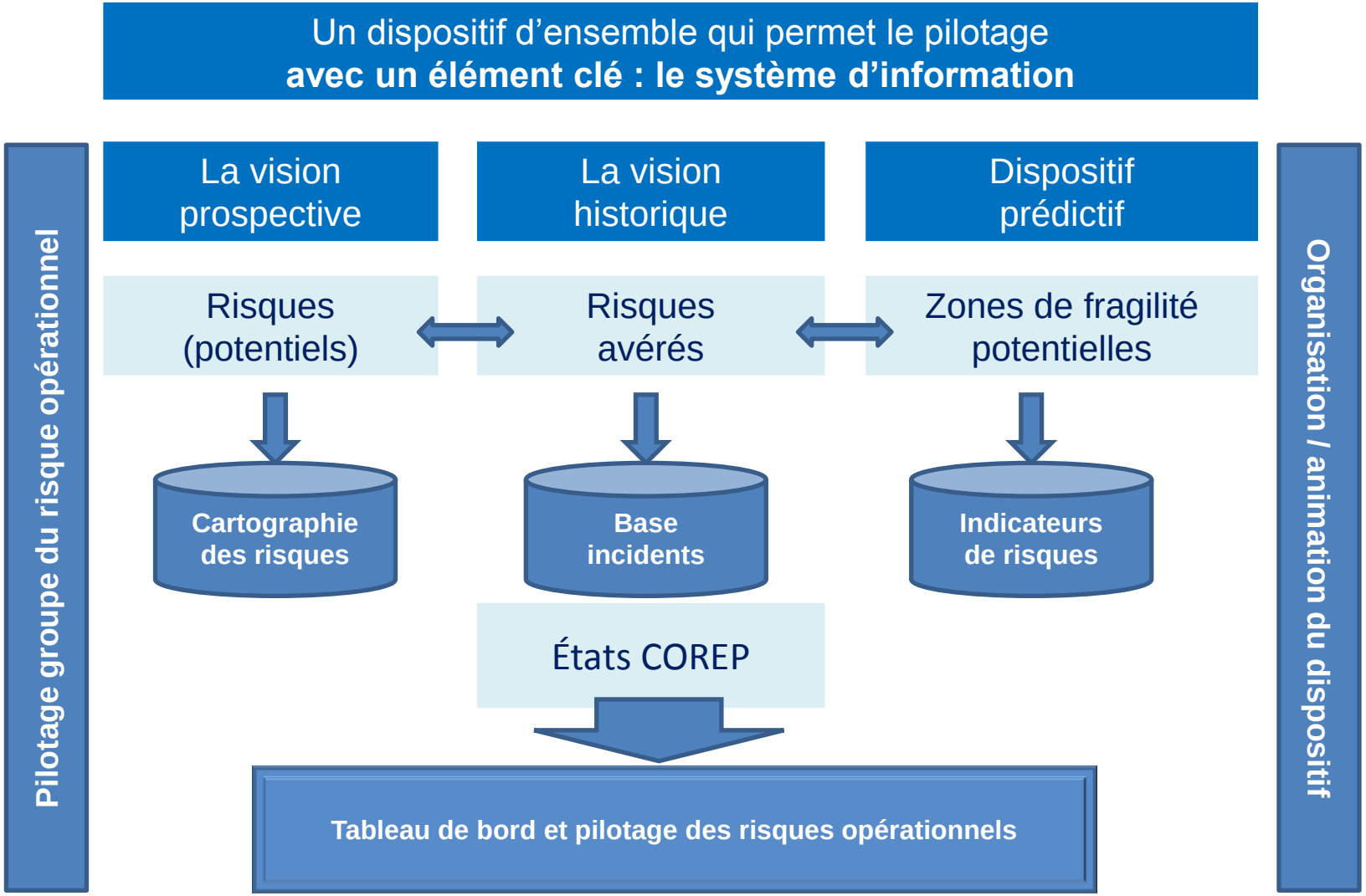
La place des risques opérationnels dans la gestion des risques et la gouvernance (3/4)

Quelle mise en œuvre ?

- Le risque opérationnel est au **cœur des dispositifs de gestion de risques** des établissement 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…),
  - concernant 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).

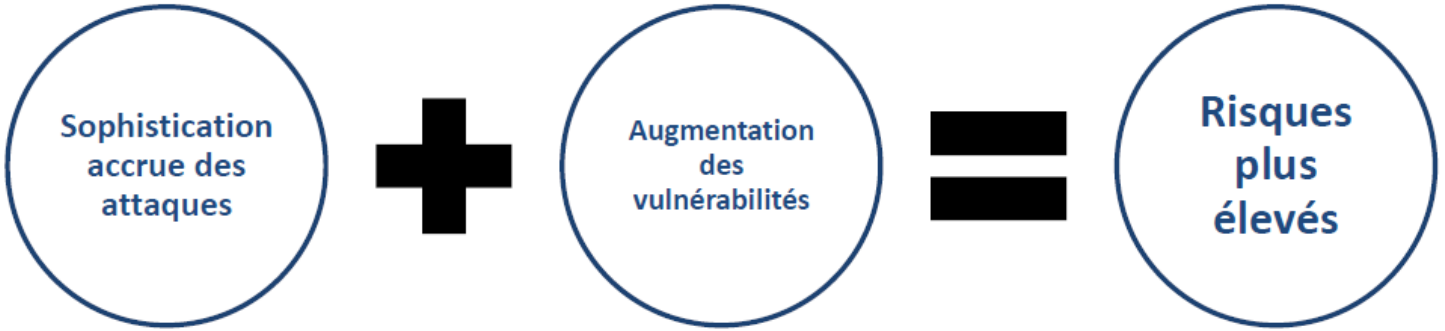
- Une attention particulière doit être portée à certaines **faiblesses** observées :
  - surveillance imparfaite du **périmètre d'activité** (entités étrangères, lignes de métier périphériques…),
  - manque de **moyens affectés au contrôle interne**,
  - prise en compte imparfaite de certains risques : ***conduct risk*** ou **risque informatique** en particulier.

2. La place des risques opérationnels dans la gestion des risques et la gouvernance (4/4)

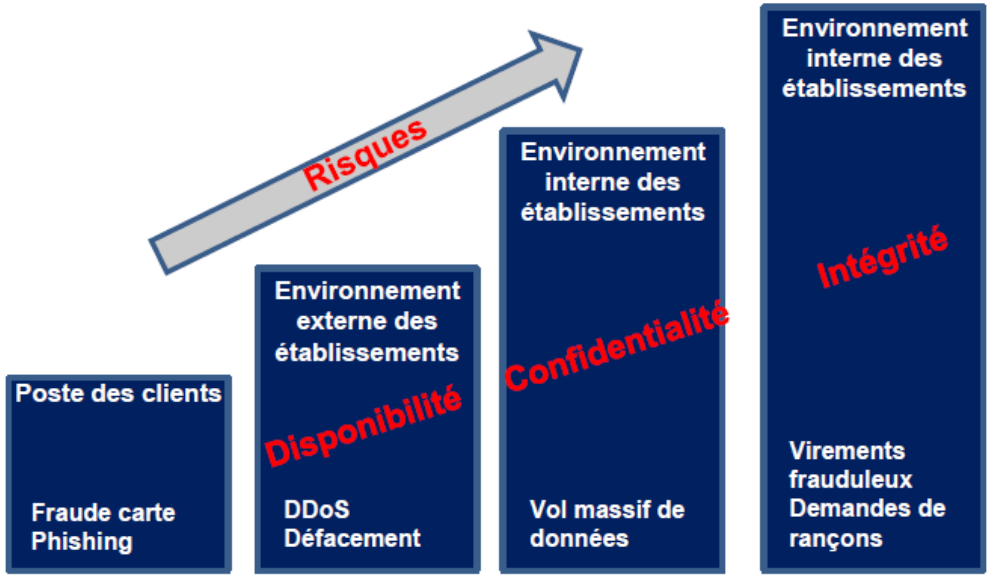


3. Un enjeu particulier : la gestion du risque informatique (1/3)

- Le risque informatique croissant renforce l'attention qui doit lui être portée



- Les systèmes des établissements sont visés
- L'impact financier augmente
- Le risque de réputation est plus fort



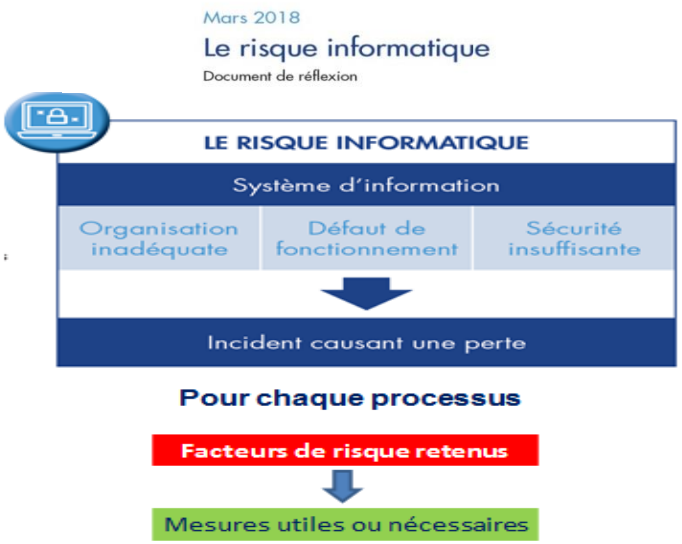
3. Un enjeu particulier : la gestion du risque informatique (2/3)

L'un des enjeux est la **meilleure prise en compte du risque informatique au sein du cadre de gestion du risque opérationnel pour le couvrir dans toute sa diversité**.

Plusieurs publications existent à son sujet, mais les références restent encore des standards techniques (NIST, ISO, …) et le cadre prudentiel du risque opérationnel doit ainsi être revu pour le prendre en compte :

	Références	Objets
Au niveau bâlois	*Guidance on cyber resilience for financial market infrastructures – juin 2016*	Neuf groupes de conseils relatifs à la gestion du cyber-risque des infrastructures de marché, références souvent également pertinentes pour les institutions financières
	Issues paper on cyber risk to the insurance sector – août 2016	Publication à vocation pédagogique afin d'initier le débat sur la gestion du risque informatique chez les organismes d'assurance et leurs superviseurs
Au niveau européen	Orientations sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (*SREP*) – mai 2017	Ensemble d'orientations que les superviseurs ont intégré dans leur procédure SREP afin de mieux surveiller le risque informatique des établissements contrôlés
	Recommandations sur l'externalisation vers des fournisseurs de services en nuage (*cloud*) – mars 2018	Ensemble de recommandations adressées tant aux établissements qu'aux superviseurs, afin de mieux encadrer le risque pris lors du recours aux prestataires de *cloud*
Au niveau national	Analyses et Synthèses de l'ACPR sur le *cloud computing – juillet 2013*	Publication de l'ACPR contenant quelques "bonnes pratiques" relatives au recours aux prestataires de *cloud*
	Document de réflexion de l'ACPR sur le risque informatique – mars 2018	Document pédagogique visant à expliquer la vision de l'ACPR à propos du risque informatique, qui a donné lieu à consultation publique afin d'échanger sur ce sujet en particulier avec les établissements supervisés

3. Un enjeu particulier : la gestion du risque informatique (3/3)



Le document de réflexion de l'ACPR sur le **risque informatique** souligne que ce risque est une **préoccupation majeure** :

- toute l'activité des établissements est dépendante de leur système d'information et ces environnements sont devenus très complexes à gérer
- les dommages informatiques peuvent avoir des conséquences particulièrement graves (pannes, cyberattaques)

Les travaux des instances internationales sur le risque informatique se sont intensifiés depuis 2015 et continuent (une analyse des pratiques de contrôle est en cours au niveau du Comité de Bâle) mais l'ancrage du risque informatique dans le risque opérationnel reste à clarifier.

Merci de votre attention
et retrouvez les analyses de l'ACPR sur notre site internet : www.acpr.banque-france.fr