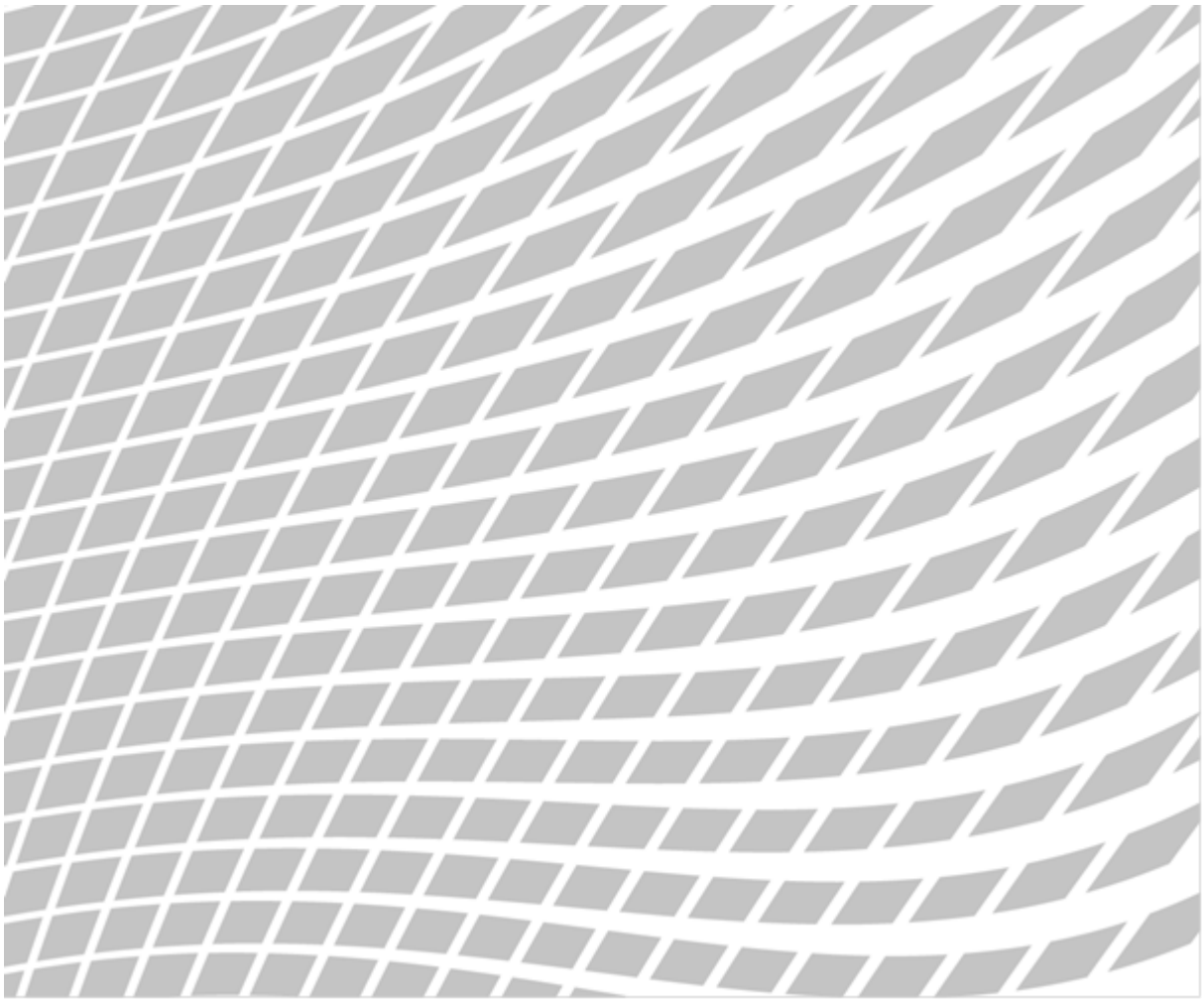
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

23 mai 2013

Révision partielle de la circulaire 2008/21 : Risques opérationnels – banques

Rapport explicatif



Einsteinstrasse 2, 3003 Berne
Tél. +41 (0)31 327 91 00, fax +41 (0)31 327 91 01
www.finma.ch

b102255-0000008

Référence : b102255-0000008

Table des matières

Référence : b102255-0000008

Eléments essentiels

1. Les graves pertes liées aux risques opérationnels observées au cours de la crise financière et durant ces dernières années ont conduit, partout dans le monde, à une réévaluation de l'importance de ce domaine de risque. Cette réévaluation a conduit, au niveau international, à l'élaboration d'exigences réglementaires qualitatives définies par le Comité de Bâle comme normes dans le document « *Principles for the Sound Management of Operational Risk* » de juin 2011. Les exigences quantitatives (en matière de fonds propres) ne sont pas concernées par la présente révision de la circulaire et demeurent inchangées.

2. Les onze principes de la réglementation précitée sont exposés dans la circulaire FINMA 2008/21 « Risques opérationnels – banques » sous la forme de six principes. Les principes qui sont particulièrement importants pour la gestion des risques opérationnels ou qui ne sont pas encore suffisamment repris dans d'autres réglementations suisses sont complétés par des explications choisies.

3. La circulaire révisée prévoit que les exigences qualitatives doivent être appliquées en tenant compte de la taille de la banque. Ainsi, les petites banques et les négociants en valeurs mobilières de la catégorie 5 de la FINMA et les banques appartenant à la catégorie 4 dont les activités d'affaires n'ont pas une complexité significative sont exemptés de l'application de certaines dispositions.

4. Outre l'adaptation des exigences qualitatives du nouveau chapitre IV. de la circulaire FINMA 2008/21, la possibilité existe désormais de définir, dans le cadre d'une annexe, des exigences très concrètes pour les risques spécifiques. De plus, le traitement des données électroniques des clients est régi dans la nouvelle annexe 3. Selon les circonstances, d'autres thèmes seront introduits à l'avenir sous cette même forme détaillée.

5. La nouvelle annexe 3 contient neuf principes et de nombreuses explications concernant la gestion adéquate des risques en rapport avec la confidentialité des données électroniques des personnes physiques (« particuliers ») dont les relations commerciales sont suivies et gérées en ou de Suisse. Ces principes traitent principalement du risque d'incidents en relation avec la confidentialité des données des clients du fait de l'utilisation de systèmes électroniques. Ils n'abordent que de manière marginale les réflexions sur la sécurité des données physiques ou les questions relatives à l'intégrité et à la disponibilité des données.

1 Contexte

1.1 Evolutions internationales

De graves pertes opérationnelles au cours de la crise financière et durant ces dernières années ont conduit, partout dans le monde, à une réévaluation des risques opérationnels. Au niveau international, des discussions ont donc été menées tant sur les exigences quantitatives que sur les exigences régulatoires qualitatives en relation avec la gestion des risques opérationnels au sein des banques. Depuis 2010, le *Standard Implementation Sub-Group for Operational Risk* (« SIGOR ») au sein duquel la FINMA est représentée travaille à la révision des exigences en capital pour les risques opérationnels, sur mandat du Comité de Bâle sur le contrôle bancaire (CBCB – *Basel Committee on Banking Supervision* « BCBS »). Dans un premier temps, les exigences en capital existantes pour les risques opérationnels ont été remises en cause et un recalibrage – qui est susceptible de conduire à des exigences en capital plus élevées, notamment pour les moyennes à grandes banques – a été envisagé. Par ailleurs, des faiblesses dans la conception de la définition de Bâle II relatives aux approches de l'indicateur de base et standard pour le calcul du capital ont été identifiées. Les discussions ne sont toutefois pas assez avancées pour qu'il existe déjà un calendrier concert pour l'intégration dans le corpus réglementaire de Bâle II. C'est pourquoi, dans un premier temps, il n'y a pas matière à adapter la circulaire FINMA 2008/21 du point de vue des exigences quantitatives.

Les principes « *Principles for the Sound Management of Operational Risk* » *(« BCBS-Principles »)* élaborés par le groupe de travail SIGOR ont valeur de nouvelle directive pour la gestion des risques opérationnels et ont été adoptés par le BCBS en 2011. Ce corpus réglementaire succède au corpus réglementaire BCBS « *Sound Practices for the Management and Supervision of Operational Risk* » (« BCBS-Practices 2003 ») datant de 2003 sur lequel se fondent les exigences qualitatives de la circulaire FINMA 2008/21 actuellement en vigueur. Dans de nombreux Etats membres du BCBS, le corpus réglementaire concernant les exigences qualitatives a déjà été implémenté, que ce soit directement comme partie intégrante de la régulation locale des risques opérationnels ou indirectement, sous la forme d'un *self assessment template*.

Le niveau insuffisamment détaillé des anciennes exigences qualitatives de base et leur domaine d'application restreints sont d'autres raisons qui ont plaidé en faveur d'une révision de la circulaire FINMA 2008/21. Conséquences de ces faiblesses, les rapports des sociétés d'audit prudentiel concernant les risques opérationnels se sont révélés peu efficaces. Il est par exemple difficile de faire la distinction entre les banques avec une bonne gestion des risques opérationnels et celles affichant des déficiences dans ce domaine. Le nombre de cas d'événements opérationnels survenus ces dernières années a, en outre, montré qu'il était nécessaire d'avoir des exigences plus différentiées à l'égard de la gestion des risques opérationnels.

1.2 Reprise des *BCBS-Principles* dans la circulaire FINMA 2008/21

Les onze *BCBS-Principles* sont exposés dans la circulaire FINMA 2008/21 « Risques opérationnels – banques » sous la forme de six principes. Les principes qui sont particulièrement importants pour la

gestion des risques opérationnels ou qui ne sont pas encore suffisamment transposés dans d'autres réglementations suisses sont complétés par des explications choisies, extraites des *BCBS-Principles*. Les redondances avec d'autres circulaires sont aussi circonscrites que possible.

La circulaire révisée prévoit que les exigences qualitatives doivent être appliquées en tenant compte de la taille de la banque. Ainsi, les petites banques et les négociants en valeurs mobilières de la catégorie 5 de la FINMA et les banques appartenant à la catégorie 4 dont les activités d'affaires n'ont pas une complexité significative sont exemptés de l'application des chiffres marginaux 124, 125, 127 let. c à i, 128, 130 à 131.

Du fait du plus grand niveau de précisions des exigences qualitatives générales qui, par ailleurs, valent désormais pour une population plus vaste de banques, les principes élargis ont désormais trouvé leur place dans le (nouveau) chapitre IV. de la circulaire FINMA 2008/21. De plus, la possibilité existe désormais de définir, dans le cadre d'une annexe, des exigences très concrètes pour les risques spécifiques. Le traitement des données électroniques des clients est ainsi régi dans la nouvelle annexe 3. Selon les circonstances, d'autres thèmes seront introduits à l'avenir sous cette même forme détaillée.

1.3 Nouvelle annexe 3 – Ajout à la circulaire FINMA des principes de bonne gestion des risques en lien avec le traitement des données électroniques du client

La garantie de la confidentialité des données des clients représentent un risque opérationnel majeur pour les banques et les négociants en valeurs mobilières en Suisse. Comme pour les autres risques opérationnels dotés d'une composante de réputation, lorsqu'il y a un trop grand écart vis-à-vis des standards de la branche, il existe une menace sérieuse non seulement pour l'établissement concerné, mais aussi pour la réputation du marché financier suisse.

La nouvelle annexe 3 présente des principes et des explications concernant la bonne gestion des risques en lien avec la confidentialité des données électroniques des personnes physiques (« particuliers ») dont les relations commerciales sont suivies et gérées en ou de Suisse. Ces principes traitent principalement du risque d'incidents en relation avec la confidentialité des données des clients du fait de l'utilisation de systèmes électroniques. Ils n'abordent que de manière marginale les réflexions sur la sécurité des données physiques ou les questions relatives à l'intégrité et à la disponibilité des données. Les dispositions juridiques fondamentales ne trouvent pas seulement leur source dans le droit de la surveillance[1], mais aussi dans la législation relative à la protection des données[2] et dans le droit civil.

L'annexe 3 comprend, en tout, neuf principes et cinquante-neuf chiffres marginaux qui ont été développés en collaboration avec des représentants de l'industrie et sont la traduction de leurs expériences avec le traitement des données des clients. Elle règle en détails la manière de procéder

[1] Notamment art. 3 et 47 LB ainsi qu'art. 9 OB ; art. 10 et 43 LBVM ainsi qu'art. 19 s. OBVM.
[2] Notamment art. 7 LPD ainsi qu'art. 8 ss OLPD (cf. également à ce sujet les guides du PFPDT ; consultables sous « http://www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=fr »).

attendue par la FINMA pour l'instauration d'un cadre global garantissant la confidentialité des données des clients. Les explications concernant les aspects relevant de la *compliance* précèdent la définition des données d'identification du client (*Client Identifying Data* – « CID »). Puis viennent les explications concernant les exigences relatives aux systèmes, processus et personnes. Enfin, l'accent est mis sur les processus de surveillance et d'identification des risques, compte tenu des risques liés à la confidentialité des CID en cas d'externalisation.

Mention est ensuite faite que les incidents en relation avec la confidentialité d'une grande quantité de données de clients peuvent résulter d'une négligence ou être causés intentionnellement. C'est pourquoi la FINMA attend qu'une attention particulière soit accordée à l'instauration à l'échelle de l'entreprise d'une prise de conscience concernant la diligence à apporter au traitement des données des clients.

Au deuxième chapitre figure un glossaire qui donne les définitions des principales notions utilisées dans l'annexe 3 de la circulaire.

1.4 Atelier consacré au présent projet de circulaire FINMA 2008/21

Les modifications de la circulaire FINMA 2008/21 «Risques opérationnels – banques» ont été présentées et débattues lors d'un atelier qui s'est tenu le 8 mars 2013 et auquel ont participé : la FINMA (présidence), l'Association suisse des banquiers, Credit Suisse AG, Deloitte SA, Ernst & Young SA, KPMG SA, PricewaterhouseCoopers SA, Raiffeisen Suisse société coopérative, RBA Holding AG, la Chambre fiduciaire, UBS SA, l'association des banques étrangères en Suisse, l'Union des Banques Cantonales Suisse, l'Association des banquiers privés suisses. Les points soulevés par les participants présents ont été consignés par la FINMA dans un procès-verbal qui a éventuellement été encore adapté. Tous les thèmes portés au procès-verbal ont été examinés ci-après par la FINMA.

2 Retour sur les futures adaptations de la circulaire FINMA 2008/21

Les règles quantitatives relatives aux risques opérationnels n'ont pas été révisées dans le cadre de Bâle III. Le calcul des exigences en fonds propres pour les risques opérationnels demeure inchangé. Pour les autres types de risques, des exigences en fonds propres relevées et/ou des exigences qualitatives plus élevées sont applicables depuis (par exemple pour les liquidités). Bien que, dans l'intervalle, le CBCB ait reconnu que les approches simples (approche de l'indicateur de base, approche standard) servant au calcul des exigences en fonds propres pour les risques opérationnels recèlent certaines faiblesses (comme le manque de sensibilité au risque de l'indicateur des revenus) et qu'il se soit attelé au remaniement des exigences quantitatives, les travaux ne sont pas encore suffisamment avancés pour qu'il soit possible de donner une planification. La FINMA transposera en temps voulu les adaptations correspondantes dans la régulation nationale, en respectant les processus usuels.

3 Vue d'ensemble des principales modifications et répercussions

L'ancienne annexe 1 « Exigences qualitatives » a été entièrement remaniée et intégrée à la circulaire, en raison de son importance, pour former le nouveau chapitre IV. Parallèlement, la structure de la circulaire a été adaptée comme le montre le tableau 1 ci-après. De ce fait, l'ancienne annexe 2, qui classifiait les segments d'affaires conformément à l'art. 93 al. 2 OFR, est devenue la nouvelle annexe 1. La vue d'ensemble pour la classification des types d'événements ne figure désormais plus dans l'annexe 3, mais dans l'annexe 2. Enfin, dans le cadre de la présente révision, la présentation dans l'annexe 3 d'un tableau de concordance permettant de comparer les dispositions de la circulaire FINMA et les standards minimaux du Comité de Bâle a été abandonnée. Ce sont, par conséquent, les nouveaux principes régissant le traitement des données électroniques des clients qui forment désormais l'annexe 3.

La révision et l'intégration des exigences qualitatives dans le corps principal de la circulaire FINMA ont également entraîné de légères modifications de la disposition relative à l'objet de la circulaire FINMA et de la définition de « Risques opérationnels » ainsi que des dispositions sur les exigences en fonds propres (nouveau chapitre III).

Ancienne structure de la circulaire FINMA	Nouvelle structure de la circulaire FINMA
I. Objet	**I. Objet**
II. Définition (art. 89 OFR)	**II. Définition**
	III. Exigences de fonds propres
III. L'approche de l'indicateur de base (BIA, art. 92 OFR)	A. Approche de l'indicateur de base (BIA, art. 92 OFR)
IV. L'approche standard (art. 93 OFR)	B. Approche standard (AS, art. 93 OFR)
A. Mécanisme	a) Mécanisme
B. Exigences générales (art. 93 al. 3 OFR)	b) Exigences générales (art. 93 al. 3 OFR)
C. Exigences supplémentaires pour les banques actives à l'étranger	-
V. Approches spécifiques aux établissements (AMA, art. 94 OFR)	C. Approches spécifiques aux établissements (AMA, art. 94 OFR)
A. Autorisation	a) Autorisation
B. Exigences qualitatives	b) Exigences qualitatives supplémentaires
C. Exigences quantitatives générales	c) Exigences quantitatives générales
D. Données internes relatives aux pertes (art. 94 al. 2 OFR)	d) Données internes relatives aux pertes (art. 94 al. 2 OFR)
E. Données externes relatives aux pertes (art. 94 al. 2 OFR)	e) Données externes relatives aux pertes (art. 94 al. 2 OFR)
F. Analyse de scénarios (art. 94 al. 2 OFR)	f) Analyse de scénarios (art. 94 al. 2 OFR)
G. Environnement d'affaires et système de contrôle interne (art. 94 al. 2 OFR)	g) Environnement d'affaires et système de contrôle interne (art. 94 al. 2 OFR)
H. Atténuation du risque par des assurances	h) Atténuation du risque par des assurances
VI. Utilisation partielle d'approches	D. Utilisation partielle d'approches
VII. Ajustements des exigences de fonds propres (art. 45 al. 3 OFR)	E. Ajustements des exigences de fonds propres (art. 45 al. 3 OFR)
	F. Fonds propres minimaux et plancher *(floor)*
Annexe 1 – Exigences qualitatives de base	**IV. Exigences qualitatives**
	A. Principe de proportionnalité
	B. Exigences qualitatives de base

	C. Exigences qualitatives spécifiques au risque
	V. Audit et évaluation par les sociétés d'audit
Annexe 2 – Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR	**Annexe 1 – Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR**
Annexe 3 – Vue d'ensemble pour la classification des types d'événements	**Annexe 2 – Vue d'ensemble pour la classification des types d'événements**
Annexe 4 – Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle	-
	Annexe 3 – Traitement des données électroniques de clients

Tableau 1

4 Explications des différentes modifications apportées à la circulaire et aux annexes

4.1 Titre et bases légales

Le sous-titre de la circulaire FINMA 2008/21 « Risques opérationnels – banques »[3] a été modifié en « Exigences de fonds propres et exigences qualitatives relatives aux risques opérationnels dans le secteur bancaire », pour mieux souligner l'importance des exigences qualitatives. Par ailleurs, l'art. 9 al. 2 OB a été ajouté aux bases légales pour garantir le lien de ces dispositions avec la gestion des risques.

4.2 Objet (Cm 1)

L'objet a été complété par la définition des exigences qualitatives de base pour la gestion des risques opérationnels conformément à l'art. 9 al. 2 OB ainsi que par la mention soulignant que les exigences qualitatives de bases correspondent aux *BCBS-Principles*.

4.3 Définition (Cm 2 et nouveau Cm 2.1)

Dans le titre, la référence à l'art. 89 OFR a été supprimée, la définition des risques opérationnels ayant été enrichie d'un paragraphe sur les risques de réputation.

[3] Anciennement « Exigences de fonds propres relatives aux risques opérationnels dans le secteur bancaire ».

4.4 Exigences de fonds propres (Cm 3 ss)

4.4.1 Approche de l'indicateur de base (BIA, art. 92 OFR)

Cm 20-22
Ces dispositions ont été supprimées dans la mesure où elles sont remplacées par le nouveau principe de proportionnalité (cf. chapitre IV. A de la circulaire).

4.4.2 Approche standard (AS, art. 93 OFR)

Cm 28
Cette disposition a été supprimée dans la mesure où elle est remplacée par le nouveau principe de proportionnalité (cf. chapitre IV. A de la circulaire).

Cm 29
Correction de la référence à la nouvelle annexe 1 (anciennement annexe 2).

Cm 30-44
Abrogés. Les chiffres marginaux 30 à 44 contenaient des exigences opératives supplémentaires pour les banques actives à l'étranger. Les exigences des anciens chiffres marginaux 30 à 44 sont intégralement comprises dans les nouvelles exigences qualitatives de base (Cm 117 ss). Le champ d'application des nouvelles exigences qualitatives dépend de la taille et de la complexité des différents établissements (Cm 117 à 118). Des activités à l'étranger contribuent à la complexité de l'établissement.

4.4.3 Approches spécifiques aux établissements (AMA, art. 94 OFR)

Cm 50
Modification du titre et du renvoi selon lequel les banques qui utilisent une approche spécifique à l'établissement doivent désormais satisfaire aux exigences qualitatives de base selon le chapitre IV.B et non plus de l'ancienne annexe 1.

Cm 64
Abrogé, (cf. les explications relatives au Cm 40 à 42 ci-avant).

Cm 71 et Cm 79
Correction de la référence à la nouvelle annexe 2 (anciennement annexe 3).

4.5 Fonds propres minimaux et plancher (*floor* ; nouveau Cm 116)

Les nouvelles dispositions relatives aux fonds propres minimaux et au plancher harmonisent la circulaire FINMA 2008/21 avec les chiffres marginaux 381 à 381.1 de la circulaire FINMA 2008/19 « Risques de crédit – banques » et ne sont déterminantes que pour les banques qui utilisent l'approche AMA.

4.6 Exigences qualitatives (nouveau Cm 117 ss)

4.6.1 Remarques préalables

En 2006, lors de l'élaboration de l'actuelle circulaire FINMA 2008/21 réalisée à l'occasion de la mise en œuvre du – à l'époque, tout nouvel – accord de Bâle sur les fonds propres (Bâle II) et concomitante à celle des circulaires FINMA 2008/19 « Risques de crédit – banques », 2008/20 « Risques de marché – banques », 2008/22 « Publication FP – banques » et 2008/23 « Répartition des risques – banques » qui étaient conçues comme des dispositions d'exécution relatives à la – à l'époque, toute nouvelle – ordonnance sur les fonds propres (OFR), seuls sept principes concernant les exigences qualitatives avaient été repris des *BCBS-Practices 2003* et les explications détaillées avaient été délibérément écartées – à la faveur des paragraphes explicatifs des *BCBS-Practices* 2003. Aujourd'hui, il apparaît que la formulation de ces principes est trop peu concrète et qu'en particulier, ils ne traitent pas ou pas suffisamment des thèmes suivants :

- analyse des données internes (ou externes) relatives aux pertes en relation avec les faiblesses systématiques de la structure de contrôle interne concernant les risques opérationnels ;
- exigences générales pour la définition et le développement continu des indicateurs de risques et de performance ou *Key Risk Indicators* (KRI) et *Key Performance Indicators* (KPI) en lien avec les risques opérationnels[4] ;
- exigence en relation avec les scénarios de risque concernant les risques opérationnels qui sont définis sur avis de l'expert (par exemple, scénarios mettant l'accent sur la sécurité des données des clients).

Comme, actuellement, les banques qui utilisent l'approche de l'indicateur de base et ne remplissent aucun des critères prévus aux chiffres marginaux 22 et 23 aujourd'hui en vigueur sont exemptées du respect des exigences qualitatives, seul un tout petit nombre de banques et de négociants en valeurs mobilières (moins de 10 % de la population des assujettis) est tenu de respecter les exigences qualitatives.

Conséquences de ces faiblesses, les rapports des sociétés d'audit prudentiel portant sur les risques opérationnels se sont révélés peu efficaces. En vertu de la réglementation actuelle, la gestion des risques opérationnels n'est jugée qu'au niveau général par les sociétés d'audit prudentiel.

[4] Par exemple, indicateurs de risques opérationnels dans le domaine des opérations de négoce non autorisées conformément aux exigences de la Communication FINMA (2011) « Opérations de négoce non autorisées ».

La circulaire révisée prévoit que les exigences qualitatives doivent être appliquées en tenant compte de la taille de la banque (cf. ci-après le principe de proportionnalité sous 4.6.2).

4.6.2 Principe de proportionnalité (Cm 117 à 118)

Les « petites banques » sont exemptées de l'application de certaines exigences qualitatives, sachant que les dispositions concernées sont signalées au niveau des chiffres marginaux. Sont qualifiées de « petites banques » au sens de la circulaire, les banques et négociants en valeurs mobilières de la catégorie 5, tous les négociants en valeurs mobilières de la catégorie 4 ainsi que les banques de la catégorie 4 qui disposent d'activités d'affaires de faible complexité. Elles sont dispensées de l'application des chiffres marginaux 124, 125, 127 let. c à i, 128, 130 à 131.

Les banques des catégories 4 et 5 de la FINMA représentent environ 90 % de la totalité de la population des assujettis. La FINMA s'attend à ce qu'en application du principe de proportionnalité, de nombreuses banques de la catégorie 4 remplissent toutes les exigences qualitatives de fonds.

4.6.3 Exigences qualitatives de base (Cm 119 ss)

Les onze *BCBS-Principles* sont désormais exposés dans la partie principale de la version révisée de la circulaire FINMA 2008/21 « Risques opérationnels – banques » sous la forme de six principes. La circulaire telle qu'elle est présentée se concentre sur les éléments que la FINMA juge essentiels pour la gestion des risques opérationnels. Les explications qui n'ont pas été reprises dans la circulaire ont en partie déjà été mises en œuvre dans le cadre d'autres réglementations (lois, ordonnances et circulaires) et n'ont donc pas été répétées dans la circulaire pour cette raison. Certaines explications des *BCBS-Principles* sont triviales, de sorte que, dans la circulaire, une réglementation explicite a été délibérément omise.

Principe 1 : responsabilités (Cm 120 à 123)

La propension au risque *(Risk Appetite)* se rapporte aux risques inhérents qu'une banque est *a priori* prête à prendre. Les mesures d'une banque destinées à restreindre ces risques (par exemple par des limites ou des réductions de risque ainsi que par la couverture des risques) et à tolérer les risques résiduels définissent sa tolérance au risque *(Risk Tolerance)*.

Une banque peut par exemple estimer que les risques opérationnels liés aux affaires transfrontières avec les clients d'un pays donné sont tels qu'elle renonce à ces dernières. Cette décision peut être justifiée par des arguments d'ordre financier ou en termes de réputation et montre que la banque n'est pas disposée à prendre de risque à ce sujet.

En revanche, une banque peut parfaitement décider d'assumer jusqu'à un certain point, les risques inhérents aux affaires transfrontalières avec les clients d'un pays donné. Dans ce cas, elle définit des règles internes pour réglementer cette activité commerciale (par exemple au moyen d'une directive interne concernant les affaires transfrontières avec les clients du pays concerné). Ces règles peuvent être plus ou moins détaillées, être descriptives ou prescriptives. Elles doivent toutefois être alignées

sur la définition de la tolérance au risque. Une banque étant toujours confrontée à des exceptions et à des erreurs (par exemple suite à des insuffisances au niveau de la formation, à un manque de ressources ou à un défaut de contrôles), elle doit préciser jusqu'à quel point ces exceptions ou ces erreurs sont tolérées, en fixant, par exemple, une valeur seuil aux dites « *Exceptions to Policy* ». Ces dernières doivent donc être relevées, contrôlées et rapportées périodiquement. En cas d'entorse à la tolérance au risque, la direction doit être informée et, le cas échéant, intervenir.

Les définitions de la propension et de la tolérance au risque peuvent répondre à des temps différents. La propension au risque étant plutôt de nature stratégique, elle est généralement considérée comme une composante tournée vers l'avenir de l'analyse des risques d'une banque. Par conséquent, la propension au risque est déterminée pour plusieurs années (par exemple, avec un horizon de deux ans). Au contraire, la tolérance au risque cible une période plus courte et est donc vérifiée à une fréquence plus soutenue et adaptée si nécessaire (par exemple, par la surveillance des limites sur une base mensuelle ou trimestrielle).

Dans l'exemple ci-avant, la banque a par ailleurs la possibilité, sur décision du conseil d'administration, de sortir des affaires transfrontières avec les clients d'un pays donné, car elle ne peut plus en assumer les risques opérationnels selon des critères de rentabilité. Logiquement, la banque n'acceptera aucun nouveau client de ce pays, mais devra continuer de travailler un certain temps avec les clients et les infrastructures existants. La banque doit toutefois continuer de respecter et de surveiller la tolérance au risque qu'elle a définie à ce sujet jusqu'au terme de la procédure de sortie de ces affaires, par exemple par la résiliation de l'ensemble des relations clients transfrontières ou par la vente de l'unité compétente à une banque tierce.

Les déclarations selon lesquelles il n'y a pas de tolérance pour les risques opérationnels appartiennent désormais au passé et ne répondent plus aux exigences relatives à la propension et à la tolérance au risque. Lorsqu'une nouvelle affaire est acceptée ou qu'un segment d'affaires continue à être exploité, des risques opérationnels apparaissent ou perdurent et sont tolérés jusqu'à un certain point tant qu'aucune décision contraire n'est prise.

Une exigence essentielle pour l'élaboration de concepts pertinents concernant les définitions de la propension et de la tolérance au risque pour les risques opérationnels est qu'il faille les définir séparément, pour chaque risque matériel (par exemple, risques liés aux affaires transfrontières, risques concernant les opérations de négoce non autorisées, *Investment Suitability*, *Business Continuity Management*, confidentialité des données des clients, etc.). De plus, les banques doivent adapter la tolérance au risque à leur propre gestion et à leurs propres structures de contrôle afin d'en assurer une surveillance et une mesure efficaces.

Principe 2 : concept cadre et système de contrôle (Cm 124 à 126)

Les risques opérationnels inhérents sont les risques opérationnels avant prise en compte des contrôles. Ils peuvent également être qualifiés de « sous-jacents » ou d'« initiaux » et évoluer dans la durée.

Par exemple, les risques opérationnels dans le domaine IT peuvent rapidement s'aggraver du fait des nouvelles technologies et méthodes d'attaque (cyberattaques). Le nombre de cas de fraude internes et le montant des dommages occasionnés peuvent fortement progresser lorsque les marges sont faibles et les marchés volatiles.

Les risques résiduels sont les risques après prise en compte des contrôles. Ils résultent de l'écart entre le risque inhérent et sa comparaison avec le système de contrôle. Par conséquent, les risques résiduels peuvent subir des modifications indépendamment de l'évolution du risque inhérent, par exemple lors de réductions des ressources affectées aux fonctions de contrôle ou lors de contrôles plus relâchés.

Périodiquement et notamment dans le cas des produits et des affaires d'importance pour la banque, des facteurs externes ne peuvent toutefois pas être immédiatement compensés par des améliorations du système de contrôle interne. Le fait de prendre en compte séparément les risques inhérents et les risques résiduels est également essentiel pour pouvoir juger à temps de la nécessité de mesures exceptionnelles.

L'exigence d'une classification uniforme des risques opérationnels matériels est en général satisfaite grâce à un barème d'évaluation des risques qui répertorie la fréquence et le montant potentiel du dommage des types d'événements. Cette classification peut être réalisée sur la base d'estimations de l'expert et par analyse des données. A la survenance d'un risque, les effets peuvent être d'ordre financier et/ou liés à la réputation. Une classification uniforme permet de soumettre aux comités de risque des rapports cohérents sur l'ensemble des risques opérationnels matériels. Par ailleurs, les décisions portant sur l'allocation des ressources, la fixation des priorités et les mesures d'atténuation du risque peuvent être étayées sur une catégorisation cohérente des risques opérationnels.

Une classification uniforme évite par exemple que les risques juridiques et les risques de *compliance* soient jugés, de manière impropre, avec les autres risques opérationnels.

Principe 3 : identification, limitation et surveillance (Cm 127 à 128)
L'identification des risques doit prendre en compte des facteurs internes et externes dans la mesure où, en général, ils sont complémentaires. Les enseignements résultant de l'analyse des pertes internes portent principalement sur le passé et peuvent être complétés par des éléments tournés vers l'avenir, comme les compilations et les analyses d'événements qui ont eu lieu dans d'autres banques comparables (ou « événements externes ») et les analyses des événements graves liées à un fort potentiel de pertes (ou « analyses de scénarios »).

Pour réaliser des évaluations des contrôles et des risques conformes au but, il faut typiquement commencer par établir un catalogue des risques inhérents qui sera ensuite complété par les estimations et les évaluations des risques. L'efficacité des contrôles sera évaluée en plus et les risques résiduels estimés (« RCSA – Risk Control Self Assessments »).

La compilation et l'analyse des données internes et externes relatives aux pertes doit répondre à un processus transparent et être documenté. Sur ce point, il est possible de profiter de l'expérience des

banques AMA. En l'occurrence, la lecture du papier SIGOR-BCBS *« Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches »* de juin 2011 est recommandée, le chapitre « Data » fournissant des informations de qualité sur la thématique des données relatives aux pertes. Concernant les données externes, il est possible de se référer en plus aux chiffres marginaux 86 à 88 de la présente circulaire.

Les analyses de scénarios peuvent être très utiles à l'ensemble des banques, et notamment aux banques qui disposent de peu de données relatives aux pertes. Il est essentiel que l'utilisation des analyses de scénarios soit en adéquation avec la définition des scénarios OpRisk dans le cadre de la planification du capital.

La mesure et la quantification du potentiel de risque ne doit pas nécessairement passer par une approche sophistiquée. Les exigences AMA peuvent toutefois servir d'indice de références des bonnes pratiques (« *Best Practice Benchmark* »). La complexité de l'approche quantitative doit notamment être dans un rapport adéquat avec les hypothèses adoptées[5]. Le rapport du potentiel de pertes quantifié aux exigences en fonds propres nécessite une approche intègre, en plus d'autres chiffres-clés, le quantile 99,9 % de la distribution des pertes sur une année.

Par exigences relatives à la fixation des prix et à la mesure de performance, il faut en général comprendre le processus d'allocation des exigences en fonds propres pour les risques opérationnels aux segments et unités d'affaires ainsi que l'évaluation de la performance des unités spécifiques ou des collaborateurs. Ainsi, l'évaluation annuelle de la performance du responsable d'une unité de négoce ne peut pas être indépendante du nombre des violations que son unité a commises à l'encontre des directives internes relatives à l'atténuation des risques en relation avec des transactions non autorisées.

Principe 4 : établissement de rapports internes et externes (Cm 129 à132)
Comme dans le troisième principe, pour l'identification des risques, les rapports internes et externes doivent fournir des éléments liés au passé comme des éléments tournés vers l'avenir (p. ex. événements externes et nouveaux risques potentiels).

Principe 5 : infrastructure technologique (Cm 133)
Les risques opérationnels dans le domaine IT ont connu une croissance exponentielle au cours des dernières années et doivent être classés, par toute banque, comme risque matériel.

Principe 6 : continuité en cas d'interruption de l'activité (Cm 134)
Des interruptions graves de l'activité sont souvent jugées par les banques de détail comme le plus grand risque opérationnel.

[5] Notamment de leur conservativité des hypothèses.

4.6.4 Exigences qualitatives spécifiques au risque (Cm 135 à 136)

La FINMA instaure ainsi la base pour publier, par thèmes regroupés en annexes, des concrétisations et des explications plus complètes sur la gestion des risques opérationnels.

4.7 Audit et évaluation par les sociétés d'audit (Cm 137)

L'audit relatif au respect des exigences en fonds propres et des exigences qualitatives pour les risques opérationnels est réalisé sur la base de la Circulaire FINMA 2013/3 « Activités d'audit ».

4.8 Annexe 1 – Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR

L'ancienne annexe 2 qui contient la classification des segments d'affaires conformément à l'art. 93 al. 2 OFR est devenue l'annexe 1, du fait de l'intégration des exigences qualitatives dans le corps de la circulaire.

Aucune modification n'a été effectuée sur le fond.

4.9 Annexe 2 – Classification des types d'événements

L'ancienne annexe 3 qui contient la vue d'ensemble pour la classification des types d'événements est devenue l'annexe 2, du fait de l'intégration des exigences qualitatives dans le corps de la circulaire.

Aucune modification n'a été effectuée sur le fond.

4.10 Nouvelle annexe 3 – Traitement des données électroniques de clients (Cm 1 à 69)

4.10.1 Remarques préalables

L'annexe 4 en vigueur actuellement qui présentait un tableau comparatif des dispositions de la circulaire FINMA et des standards minimaux du Comité de Bâle a été purement et simplement supprimée dans la version révisée de la circulaire FINMA 2008/21,

La nouvelle annexe 3 contient les neuf principes, ainsi que les explications y afférentes, pour la gestion adéquate des risques en rapport avec la confidentialité des données électroniques des personnes physiques ayant la Suisse comme centre de comptabilisation et ayant signé un contrat soumis au droit et aux prescriptions suisses. Ici, l'accent est mis sur le risque d'incidents en relation avec la confidentialité des données des clients du fait de l'utilisation de systèmes électroniques. Les réflexions sur la sécurité des données physiques ainsi que les dispositions relatives à l'intégrité et à la disponibilité des données ne font l'objet que de mentions marginales.

4.10.2 Champ d'application et principe de proportionnalité (Cm 1 à 2)

Les petites[6] banques sont exemptées de la mise en œuvre des chiffres marginaux suivants :

- les chiffres marginaux 15 à 19, ainsi que 24 à 29 du principe 3 ;
- tous les chiffres marginaux des principes 4 à 6 ;
- le chiffre marginal 48 du principe 7.

4.10.3 Principes de bonne gestion des risques en lien avec la confidentialité des données des clients (Cm 3 à 59)

Principe 1 : gouvernance (Cm 3 à 7)

La création d'une fonction de contrôle indépendante chargée de créer et de préserver les conditions cadres garantissant la confidentialité des données des clients est essentielle. Le traitement des données des clients est généralement assuré en grande partie par des spécialistes IT internes ou des tiers. Ces derniers doivent, en conséquence, être assujettis à la surveillance d'une unité indépendante (par exemple, d'une partie de l'organisation de contrôle des risques) pour ce qui est du respect des conditions cadres garantissant la confidentialité des données des clients. L'indépendance de la fonction de contrôle sert également à garantir des structures efficaces de remontée des informations et à identifier en continu les possibilités d'amélioration du concept cadre garantissant la confidentialité des données des clients.

Une répartition claire des responsabilités permet de pouvoir réagir rapidement, en tout temps et sur l'ensemble des sites, à d'éventuels incidents. Cela est d'une importance centrale pour une gestion efficace des risques en rapport avec des données de clients. Pour instituer de la clarté au niveau des responsabilités et pouvoir les mettre en œuvre avec cohérence, un concept cadre formel et complet sur les activités, les processus et les systèmes est requis.

Principe 2 : données d'identification du client (*Client Identifying Data*, CID; Cm 8 à 14)

Le nombre et la diversité des données de clients qu'un établissement doit traiter peuvent être très importants. L'exigence de base qui consiste à être capable de déterminer dans cette quantité de données de clients celle qui servira à son identification est partie intégrante d'un concept cadre solide et doit être respectée de tout établissement.

La définition des données d'identification des clients et leur classification est une tâche spécifique à l'établissement dans la mesure où les banques disposent d'informations différentes selon leurs modèles d'affaires, leurs produits, leurs prestations de services et leurs sites. Par exemple, un

[6] Cf. Cm 118 du chapitre IV. A.

établissement qui s'est spécialisé dans le traitement des flux de paiement aura à gérer des données de transaction en plus grande quantité qu'un établissement hypothécaire qui devra lui-même s'occuper des données de clients différentes de celles d'un établissement de gestion de fortune. Dans la définition des CID spécifique aux établissements, il convient en outre de tenir compte des incidents spécifiques à ces derniers (comme la fuite de données de clients).

L'identification des unités responsables des CID (« Data Owners ») – en règle générale, des unités commerciales familiarisés avec les clients et les données de clients spécifiques – contribue à éviter que des fonctions de services (telles que les IT) répondent seules de l'intégralité et de la cohérence de la classification.

Principe 3 : lieu de stockage et accès aux données (Cm 15 à 29) et principe 4 : normes de sécurité liées à l'infrastructure et à la technologie (Cm 30 à 36)

Une fois réglée la question préliminaire des données de clients dont dispose une banque, le troisième principe est consacré aux questions qui en découlent, à savoir du lieu où sont localisées les données des clients et de la manière dont elles doivent être protégées.

Les expériences tirées de différents incidents montrent que les enquêtes en cas de pertes de données à la suite d'opérations illégales s'orientent en premier lieu vers l'identification de la source des données. L'identification de la source des données en temps utile n'est possible que lorsqu'il existe une liste à jour des applications et des collaborateurs (tiers compris) qui ont accès aux CID. Si les investigations permettent d'exclure toute source interne, des sources externes (par exemple, une cyberattaque) sont envisagées.

Le stockage des CID à l'étranger et l'accès aux CID depuis l'étranger ne posent problème que lorsque les risques accrus qui en découlent ne sont pas compensés par un relèvement adéquat des dispositions en matière de sécurité et de transparence. Les observations issues de la pratique et de la branche quant aux différentes méthodes de protection des données à l'étranger (anonymisation, pseudonymisation, chiffrement, etc.) montrent que les processus peuvent être évalués différemment. Par exemple, pour les données pseudonymisées, le stockage des tableaux de concordance dans un environnement sûr en Suisse est considéré comme une précaution appropriée. Concernant l'obligation « d'informer les clients par courrier spécial du stockage des données à l'étranger », la consultation avec le Préposé fédéral à la protection des données et à la transparence (PFPDT) a montré que seules des « données anonymisées » permettaient véritablement de ne pas remonter à l'identité des clients concernés (irréversibilité) au sens du Cm 23.

Le principe du « Need-to-Know » est une exigence essentielle en vue d'encourager une prise de conscience à l'échelle de l'entreprise concernant le traitement des données des clients et la reconnaissance des CID comme « asset ».

Les exigences techniques en matière de normes de sécurité qui font l'objet du quatrième principe sont délibérément formulées de manière très générique afin de permettre, d'une part, l'instauration de solutions spécifiques à l'établissement et de réduire, d'autre part, les références datées autant que

faire se peut. N'en demeure pas moins l'exigence (globalement valable pour toutes les solutions IT) de comparer régulièrement ses propres normes de sécurité à la pratique du marché (au sens du « développement technique » tel que défini dans l'art. 8 al. 2 let. d de l'Ordonnance relative à la loi fédérale sur la protection des données [RS 235.11]). Pour garantir la réalisation de telles comparaisons, il faut compter en premier lieu sur le savoir-faire des spécialistes internes qui doivent être en mesure d'établir si des inputs externes sont nécessaires.

Principe 5 : sélection, surveillance et formation des collaborateurs qui ont accès aux CID (Cm 37 à 42)

Les quatre premiers principes recouvrent des exigences en matière d'organisation et d'infrastructure afin que seuls les collaborateurs et tiers autorisés aient accès à des CID. Un établissement doit par ailleurs s'assurer que les collaborateurs autorisés à traiter des CID en masse soient sélectionnés, formés et surveillés avec soin. Il est attendu des banques qu'elles s'entourent de dispositifs de protection vis-à-vis du « facteur humain », au cœur du cinquième principe, au moins équivalents à ceux de nature technique. C'est à dessein que la FINMA n'édicte pas de mesures concrètes à ce sujet.

Principe 6 : identification et contrôle des risques en relation avec la confidentialité des CID (Cm 43 à 45) et principe 7 : limitation du risque en relation avec la confidentialité des CID (Cm 46 à 48)

La thématique de la « confidentialité des données des clients » qui est au centre de l'annexe 3 de la circulaire 2008/21 révisée peut en principe être abordée selon deux perspectives :

- la perspective organisationnelle : élaboration d'exigences minimales pour créer un concept cadre adéquat pour garantir la confidentialité des données des clients. C'est cette approche qu'a suivi la FINMA pour développer l'annexe 3.
- la perspective des risques et des contrôles – établissement de scénarios concrets qui peuvent mener à une violation de la confidentialité des CID ainsi que de contrôles qui réduisent ces risques. Cette approche conduit à un degré de précision plus poussé et plus spécifique et a été adoptée par l'Association suisse des banquiers pour développer le document « Data Leakage Protection »[7] d'octobre 2012.

Les deux approches sont équivalentes et doivent être considérées comme complémentaires. Le sixième principe constitue le trait d'union entre ces approches.

Le septième principe formule l'attente de la FINMA qui entend que les activités au cours desquelles de grandes quantités de CID sont modifiées ou migrées (par exemple en raison des avancées

[7] Les pratiques du marché concernant les scénarios relatifs à la sécurité et les contrôles clés y afférents sont traités de manière approfondie par l'Association suisse des banquiers sous le titre « Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association » (octobre 2012).

technologiques ou de restructurations organisationnelles) fassent partie intégrante des scénarios de risque mentionnés ci-avant.

Principe 8 : incidents en rapport avec la confidentialité des CID, communication interne et externe (Cm 49 à 51)

Au cours de la phase de clarification d'un incident ou après la conclusion des enquêtes préliminaires, la FINMA, les autorités de poursuite pénale et les clients concernés peuvent aider la banque à limiter les conséquences financières et celles liées à la réputation. Dans ce contexte, il faut que la banque dispose d'une stratégie de communication claire.

Principe 9 : externalisation d'activités et prestations de services à grande échelle traitant des CID (Cm 54 à 59)

Dans les petites banques, en particulier, l'exposition au risque lié au traitement des données dépend fortement des standards de confidentialité de leurs prestataires externalisés. Tous les prestataires n'ayant pas les mêmes standards, la banque doit prendre en compte de manière adéquate la confidentialité des CID lors du processus de sélection et de renouvellement de tout prestataire externalisé.

4.10.4 Glossaire (Cm 60 à 67) et exemple de données d'identification du client (Cm 68)

Les données d'identification du client (*Client Identifying Data*, CID) correspondent à tous les éléments de données au sens de l'art. 3 let. a LPD qui peuvent être utilisés pour désigner ou identifier directement un client ou qui peuvent permettre, par recoupement de plusieurs éléments de données ou de sources d'informations ou encore par observation des éléments de données sur une certaine durée, de remonter à l'identité d'un client (pour les exemples, cf. chapitre III de l'annexe 3, al. 69).

5 Effets de la révision partielle

Cette révision partielle de la circulaire n'a pas d'effet sur les exigences de fonds propres[8] pour les risques opérationnels des banques et des négociants en valeurs mobilières.

Cependant, en raison des exigences qualitatives supérieures valables pour la gestion des risques opérationnels qui entreront en vigueur avec cette révision partielle, il faut s'attendre aux répercussions suivantes :

[8] Le nouveau chiffre marginal 116 concernant le « régime de floor » harmonise la circulaire FINMA 2008/21 avec les chiffres marginaux 381 et 381.1 de la circulaire FINMA 2008/19 « Risques de crédit – banques » et n'est déterminant que pour les banques AMA. Toutefois, cette disposition n'a actuellement aucun effet quantitatif sur les banques AMA.

- **Exigences qualitatives de base (chapitre IV.B)** : pour les banques, les répercussions organisationnelles et financières des exigences qualitatives de base actualisées sont minimes. S'agissant des banques des catégories 1 à 3 de la FINMA qui doivent remplir toutes les exigences sans exception, la nécessité matérielle d'agir ne sera sensible que pour les banques qui n'ont pas prêté suffisamment attention à la gestion des risques opérationnels au cours des dernières années.

  Les adaptations des exigences de base qui reposent sur les *BCBS-Principles* portent la régulation des risques opérationnels en Suisse au même niveau que celle d'autres pays. Cette révision des exigences qualitatives de base tient en outre compte de la nécessité d'améliorer la régulation en réponse à une tendance négative qui a vu éclore un nombre croissant de cas avec des pertes opérationnelles élevées. Parallèlement à ces améliorations qualitatives, la circulaire remaniée envoie un signal concernant la mise en place de structures de conduite appropriées et de mécanismes de contrôle spécifiques aux risques opérationnels.

- **Traitement des données électroniques de clients (annexe 3)** : pour les banques, les répercussions organisationnelles et financières des nouvelles exigences qualitatives en rapport avec le traitement des données de clients doivent être considérées comme matérielles. Des répercussions marginales ne sont attendues que pour les banques qui ont déjà introduit à grande échelle des mesures spécifiques aux établissements dans une logique proactive ou en raison d'incidents concrets pour répondre aux exigences de l'annexe 3. En revanche, les banques qui ont eu tendance à investir moins que la moyenne dans le savoir-faire et l'infrastructure en lien avec la protection de la confidentialité des données des clients devront combler davantage de lacunes.

  Globalement, l'implémentation de ces exigences va réduire l'ampleur des risques en relation avec les données des clients en Suisse et rapprocher les exigences prudentielles de celles d'autres pays[9] qui misent sur des valeurs comparables de la place financière (p. ex. gestion de la fortune Best-in-Class).

6 Prochaines étapes

L'entrée en vigueur de la Circ.-FINMA 2008/21 révisée est prévue le 1er janvier 2015, une fois l'audition achevée. Les dispositions relatives au plancher (cf. Cm 116) sont immédiatement applicables.

[9] Par exemple : UK FSA « Data Security in Financial Services » (avril 2008) ou Singapore MAS « Technology Risk Management Guidelines » (juin 2012).