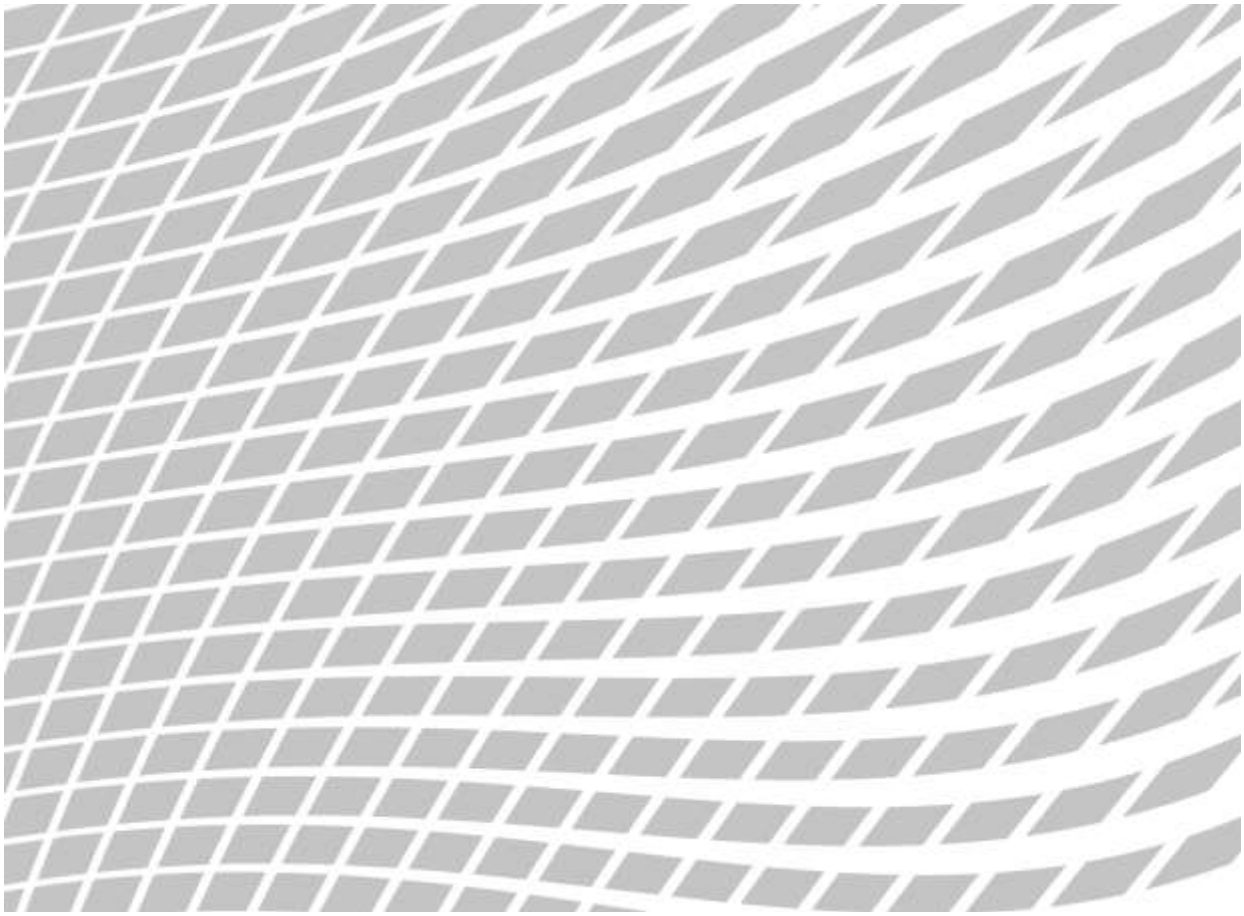
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

29 août 2013

Révision partielle de la circulaire FINMA 2008/21 « Risques opérationnels – banques »

Rapport de la FINMA sur les résultats de l'audition relative au projet de révision partielle de la circulaire « Risques opérationnels – banques », qui a eu lieu du 23 mai 2013 au 1er juillet 2013



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

A225834/00097/1046297

Table des matières

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. Ces 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 Circ.-FINMA 08/21, la possibilité existe désormais de fixer, dans le cadre d'une annexe, des exigences très concrètes pour les risques spécifiques. Le traitement des données électroniques des clients est détaillé dans la nouvelle annexe 3. La même précision sera apportée aux autres thèmes susceptibles d'être introduits à l'avenir en tenant compte du processus régulatoire (audition) alors valable.

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 Introduction

Du 23 mai 2013 au 1er juillet 2013, la FINMA a mené une audition publique ouverte aux assujettis et aux autres cercles intéressés sur le projet de révision partielle de la circulaire FINMA 2008/21 « Risques opérationnels – banques ». L'invitation à prendre part à l'audition a été publiée sur le site Internet de la FINMA ; le cercle des participants était donc ouvert.

Le présent rapport résume les prises de position des participants à l'audition relative au projet de circulaire FINMA et en donne une évaluation.

2 Prises de position reçues

La FINMA a reçu une prise de position écrite des associations et établissements suivants (par ordre alphabétique) qui ont consenti à ce qu'elle soit publiée :

- Association de Banques Suisses Commerciales et de Gestion (BCG)
- Association des banques étrangères en Suisse (AFBS)
- Association des Banquiers Privés Suisses (ABPS)
- Association suisse des banquiers (ASB)
- Banque cantonale de Zurich (ZKB)
- Chambre fiduciaire
- Credit Suisse
- HSBC
- PostFinance
- Raiffeisen
- SIX Securities Services (SIX)
- UBS
- Union des Banques Cantonales Suisses (UBCS)

3 Résultats de l'audition et évaluation par la FINMA

La révision partielle de la circulaire met l'accent sur deux thèmes spécifiques : les exigences qualitatives de base (chapitre IV.B) et le traitement des données électroniques de clients (annexe 3).

3.1 Exigences qualitatives de base (chapitre IV.B), y compris le principe de proportionnalité (chapitre IV.A), et introduction d'exigences qualitatives spécifiques au risque (IV.C)

Critique générale

La FINMA n'a pas été en mesure d'identifier une critique de fond claire concernant les exigences qualitatives de base. Le seul élément qui ressort dans la mesure où il a été évoqué dans plusieurs prises de position concerne le souhait d'une précision de la terminologie et des définitions. La FINMA a répondu ponctuellement à cette attente ; en revanche, elle n'a pas donné suite à l'établissement d'un glossaire. La FINMA recommande aux établissements de donner, à leur niveau, une définition et une interprétation des termes tels que « évaluation du risque », « classification », « limite pour les risques » et « valeur-seuil » en tenant compte de la compréhension générale de la branche.

Autre critique

Par ailleurs, les prises de position reçues concernaient pour l'essentiel les points suivants :

- Principe de proportionnalité (Cm 117[1], 118)
- Propension et tolérance au risque (Cm 120)
- Rôle de la direction opérationnelle dans le développement du concept cadre (Cm 121)
- Unité pour la gestion des risques opérationnels (Cm 122)
- Fixation des valeurs-seuils et des limites (Cm 125)
- Instruments et méthodes (Cm 127)
- Etablissement de rapports internes / événements externes (Cm 130)
- Politique de déclaration (Cm 131, 132)
- Infrastructure technologique (Cm 133)
- Exigences qualitatives spécifiques au risque (Cm 135, 136)

D'autres propositions d'adaptation de moindre importance ont été reprises, sans donner lieu toutefois à un commentaire particulier dans le présent rapport.

3.1.1 Principe de proportionnalité (Cm 117, 118, 119)

Prises de position (résumées)

- Le Cm 118 définit quels établissements sont qualifiés de « petites banques » au sens du Cm 117. Sur ce point, plusieurs prises de position ont estimé que le critère de taille d'une part et la formulation « activités d'affaires n'ayant pas une complexité significative » étaient trop restric-

[1] **Les références aux chiffres marginaux renvoient à ceux de la version soumise à audition.**

tifs et ont proposé un alignement sur les concepts de la Circ.-FINMA 13/6 « Liquidité – banques ».

- La Chambre fiduciaire note en outre un besoin de clarification pour les deux points suivants : 1) Quel organe des banques appartenant à la catégorie 4 jugera et décidera de la présence ou de l'absence d'une « complexité significative » et 2) A quelle date et de quelle manière faudra-t-il convenir avec la FINMA de la classification d'une banque de la catégorie 4 comme « n'ayant pas une complexité significative » ?

Appréciation

La FINMA a élargi les critères pour la classification des banques appartenant à la catégorie 4 de la FINMA ; désormais, l'évaluation doit prendre en compte non seulement la complexité, mais aussi la nature, l'étendue et le degré de risque des activités de l'établissement.

Pour ce qui est de l'application du principe de proportionnalité visé au Cm 117 et 118, la FINMA suit le même processus que celui stipulé dans la Circ.-FINMA 13/6 « Liquidité – banques »[2]. La FINMA laisse en premier lieu à la banque et à la société d'audit le soin d'évaluer si l'établissement satisfait aux critères. La FINMA n'en suivra pas moins d'un œil critique l'implémentation du principe de proportionnalité. La FINMA pose comme exigence de base que l'évaluation par la banque et par la société d'audit soit documentée de manière compréhensible et transparente.

La FINMA laisse les banques libres de désigner l'organe décisionnaire qui procédera à l'évaluation de la complexité et des autres critères. Cependant, pour des raisons de cohérence notamment (cf. approbation de la propension et de la tolérance au risque au Cm 120), le conseil d'administration semble le mieux indiqué pour accomplir cette tâche.

Le Cm 118 a été remanié en conséquence.

Conclusion

La FINMA a remanié les Cm 117 à 119 par analogie. Les explications ci-avant offrent en outre une ligne directrice aux établissements et aux sociétés d'audit.

3.1.2 Propension et tolérance au risque (Cm 120)

Prises de position (résumées)

- Plusieurs prises de position ont exprimé le besoin que les concepts de « nature », « type » et « niveau » soient précisés.

[2] Un processus uniforme ou semblable ne doit pas obligatoirement conduire à une conclusion identique ; une qualification différente dans le cadre des deux circulaires est possible.

- Plusieurs prises de position ont proposé des changements dans les responsabilités concernant notamment le développement et l'approbation du concept cadre.

Appréciation

Le rapport explicatif souligne les points suivants : « 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 ex. 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 ».

Ceux des établissements qui n'ont pas développé leurs définitions propres pour les principaux risques opérationnels et ont besoin d'explications plus approfondies que celles données dans le rapport explicatif, peuvent se faire une idée des concepts de « nature » et « niveau » en consultant l'annexe 2 de la circulaire (« Vue d'ensemble pour la classification des types d'événements », et notamment les sous-catégories des niveaux 2 et 3 et peuvent interpréter le concept de « niveau » au sens de « groupe ».

De légères adaptations des responsabilités ont été apportées à la version partiellement révisée de la Circ.-FINMA 08/21 dans le sens où elle autorise que le développement du concept cadre soit mené par un comité sous la conduite d'un membre de la direction opérationnelle.

Conclusion

Une légère adaptation a, d'une part, été apportée au domaine des responsabilités et, d'autre part, les questions soulevées dans le cadre de l'audition ont été commentées dans le présent rapport d'audition.

3.1.3 Rôle de la direction opérationnelle dans le développement du concept cadre (Cm 121)

Prises de position (résumées)

- Concernant le développement du concept cadre, l'ASB s'est prononcée en faveur d'un alignement de la formulation relative aux responsabilités de la direction opérationnelle sur la Circ.-FINMA 13/6 « Liquidité – banques ».

Appréciation

La FINMA salue cette proposition d'adapter les formulations.

Conclusion

La FINMA a remanié le Cm 121 par analogie.

3.1.4 Fonction pour la gestion des risques opérationnels (Cm 122)

Prises de position (résumées)

- Dans sa prise de position, Credit Suisse (comme une partie des autres participants) recommande de préciser le rôle de la direction opérationnelle lors de la définition des responsabilités et d'attribuer les compétences visées dans ce Cm non pas à une « fonction », mais à une « unité organisationnelle ».

- La Chambre fiduciaire recommande de préciser dans la circulaire si la « fonction de gestion des risques opérationnels » doit obligatoirement être distincte du « contrôle des risques » au sens des Cm 113 à 125 de la Circ.-FINMA 08/24 « Surveillance et contrôle interne – banques » ou s'il faut qu'il existe une séparation complète des fonctions.

Appréciation

La question de la Chambre fiduciaire est compréhensible et d'une grande pertinence. Remarque : dans la mesure où, en pratique, les termes de « contrôle des risques » et de « gestion des risques » sont utilisés de manière inconsistante , nous renonçons à y faire appel dans les explications suivantes.

La FINMA attend que la fonction citée au Cm 122 (désormais « unité organisationnelle ») ait non seulement recours à des instruments et méthodes « orientés vers le passé » (par ex. projets d'atténuation des risques qui ont déjà été mis en œuvre lors d'incidents opérationnels ; réalisation du contrôle des risques déjà identifiés) mais intègre également des éléments nouveaux et prospectifs au sein du concept cadre (par ex. réflexions sur la cybercriminalité, exposition croissance aux litiges juridiques, vue d'ensemble de l'exposition aux risques et estimation du potentiel de perte). Ces différentes « perspectives » et donc les différents instruments et méthodes qu'elles impliquent requièrent des modes de pensées complémentaires, et éventuellement des formations différenciées.

D'un point de vue organisationnel et contrairement à la gestion des risques de marché ou de crédit[3], la « fonction de gestion des risques opérationnels » comme le contrôle des risques appartiennent à la « deuxième ligne de défense ». C'est la raison pour laquelle il est possible d'envisager aussi bien le regroupement des deux « unités organisationnelles » au sein d'une seule unité que la séparation en unités distinctes (solution plus souple pour les banques les plus importantes). Pour mettre en place leur organisation en la matière, les établissements ont le libre choix des méthodes, instruments, formations, etc. qu'ils doivent adopter pour y parvenir.

Conclusion

Le Cm 122 a été remanié.

[3] La gestion des risques au sens de pilotage des risques/positions est souvent une tâche de la ligne.

3.1.5 Fixation des valeurs-seuils et des limites (Cm 125)

Prises de position (résumées)

- Diverses prises de position demandent une plus grande intelligibilité et/ou harmonisation des définitions.

- Au sujet de la fixation des limites / valeurs-seuils, l'ASB note en particulier que « ces limites ou valeurs-seuils, ne doivent pas être vues comme une autorisation à faire usage de ces limites comme c'est le cas avec les autres types de risque, mais au contraire comme la valeur-seuil maximale tolérable qui, si elle est franchie, déclenche les contre-mesures et les mécanismes d'établissement de rapports définis au préalable ».

Appréciation

Les définitions ont été examinées et ponctuellement adaptées. Les principales modifications concernent ici l'abandon de la mention explicite de la définition des instruments de « mesure » des risques opérationnels (pour en savoir plus à ce sujet, voir aussi Cm 127) ainsi qu'un regroupement des exigences en matière d'établissement des rapports en un point de la liste. Toutes les propositions d'adaptation n'ont pas été retenues dans la mesure où la différenciation des définitions est appropriée du fait des contextes différents auxquels se réfère chacun des points de la liste.

La FINMA partage l'appréciation que fait l'ASB des limites / valeurs-seuils. Dans sa formulation actuelle, le Cm 125 ne semble pas la contredire.

Conclusion

Le Cm 125 a été ponctuellement remanié.

3.1.6 Instruments et méthodes (Cm 127)

Prises de position (résumées)

- Plusieurs prises de position ont souligné des imprécisions concernant les exigences de base découlant du présent Cm. L'exception faite aux petites banques en vertu du Cm 119 ne serait pas nécessaire dans la mesure où les points énumérés au Cm 127 ne constituent que des « exemples » (non contraignants).

- La BCG et la ZKB ont exprimé leurs interrogations sur le choix des termes employés au point h) « mesure et quantification » et sur les exigences ou attentes générales en matière de quantification des risques opérationnels (par ex. au moyen de modèles complexes).

Appréciation

Les imprécisions concernant les exigences de base découlant du Cm 127 ont été levées en séparant les exigences obligatoires au nouveau Cm 128 des autres facteurs qui peuvent donner à de (possibles) contrôles au sein des banques qui ne sont pas qualifiées de petites (en vertu du Cm 118) et qui sont regroupés au nouveau Cm 129 ainsi qu'en adoptant de nouvelles formulations.

Quant au point soulevé par la BCG et la ZKB concernant h), il est possible de se référer au rapport explicatif : « 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[4]. »

Le commentaire dans le rapport explicatif a parfois donné l'impression aux établissements qu'on attendait d'eux des approches sophistiquées. Ce Cm ne postule pas la quantification du potentiel de perte pour toutes les banques au moyen de procédures statistiques complexes. Les estimations des experts (par ex. analyses de scénarios) peuvent, par exemple, tout aussi bien permettre une quantification suffisante du potentiel de perte. Quoi qu'il en soit, si des cas individuels sont agrégés en vue de définir le potentiel de perte total, il faut soit prendre des hypothèses conservatrices, fondées sur des estimations d'experts, soit utiliser une procédure alternative fondée sur des statistiques.

Afin d'améliorer la compréhension des termes « limitation » et « surveillance » employés dans le titre du principe, le nouveau Cm 130 contient désormais une référence au concept cadre que doit élaborer l'établissement. Par ailleurs, la fixation des prix *(pricing)* et la mesure de la performance qui figurent toutes deux dans le projet de circulaire ont été évoquées comme possibles mesures indirectes pour limiter les risques opérationnels.

Conclusion

Le Cm 127 a été scindé en deux chiffres marginaux et l'applicabilité en lien avec le principe de proportionnalité ainsi que la formulation du point h) ont été revues.

3.1.7 Etablissement de rapports internes/ événements externes (Cm 130)

Prises de position (résumées)

- Diverses prises de position demandent des reformulations ponctuelles.
- Plusieurs prises de position demandent une reformulation et une modération du point c).

[4] Notamment de la conservativité des hypothèses.

Appréciation

Le Cm 130 vise à ce que les établissements identifient les événements qui sont pertinents pour eux ainsi que les événements qui sortent de l'ordinaire (comme par ex. les affaires transfrontières avec les Etats-Unis, les rétrocessions ATF ainsi que les pertes ou les litiges juridiques ouverts auprès des homologues) et évaluent les conséquences qui en découleraient pour eux avant de définir les mesures nécessaires. L'identification de tels événements peut intervenir de différentes manières : du suivi des médias à la collecte d'événements ou de données sur les pertes anonymisés en provenance d'établissements tiers. Cette dernière tâche pourrait éventuellement être confiée à une association professionnelle sur mandat de ses membres.

Conclusion

Le Cm 130 a été ponctuellement remanié.

3.1.8 Politique de déclaration (Cm 131, 132)

Prises de position (résumées)

- Plusieurs prises de position émettent des critiques sur la proposition instaurant une politique de déclaration formelle.

- L'ASB demande une adaptation des informations à déclarer voire des exigences concernant ces informations.

Appréciation

Les exigences en matière de déclaration ont en effet été renforcées par rapport à celles existant pour d'autres types de risque. Il faut y voir l'expression d'une tendance internationale à l'extension des obligations de déclarer. La FINMA part du principe que les normes concernant les autres types de risque seront également renforcées à l'avenir.

Conclusion

Le Cm 131 a été raccourci afin d'obtenir une formulation simple et claire des exigences.

3.1.9 Infrastructure technologique (Cm 133)

Prises de position (résumées)

- Plusieurs prises de position se sont montrées critiques à l'égard de la teneur et de la formulation du Cm 133, cette dernière étant notamment perçue comme trop générale.

Appréciation

La perception du présent Cm comme étant ambigu semble justifiée. Ce Cm a pour vocation de souligner l'importance des technologies de l'information (TI) dans la couverture des besoins opérationnels et dans l'atténuation des risques opérationnels. Parallèlement, le Cm 133 met en avant la responsabilité de la direction opérationnelle en réclamant que l'attention voulue soit portée aux questions liées à l'infrastructure technologique.

Conclusion

Le Cm 133 a été remanié.

3.1.10 Exigences qualitatives spécifiques au risque (Cm 135, 136)

Prises de position (résumées)

- Cm 135 : plusieurs prises de position critiquent le manque de concrétisation de ces autres exigences et demandent leur suppression pure et simple.

- Cm 136 : plusieurs prises de position déplorent que l'actuelle formulation laisse à la FINMA la liberté d'introduire ou de concrétiser des exigences qualitatives plus poussées. Elles demandent la suppression pure et simple du présent Cm et le respect de la procédure régulière d'audition pour ces autres exigences.

Appréciation

Le Cm 135 a été enrichi de la précision selon laquelle les risques opérationnels évoqués sont des risques de grande envergure. Pour ce qui est des mesures, leur responsabilité incombe à la direction opérationnelle et des indications plus détaillées sont faites à ce sujet (mesures « complémentaires » ou « renforcer les mesures existantes »). Il a été décidé de ne pas préciser les mesures envisageables dans le cadre de la circulaire ; selon la FINMA, elles pourraient se concrétiser par un raccourcissement de la fréquence des rapports, la remise des rapports à un échelon plus élevé, une plus grande attention du management ou un traitement de ces questions à un niveau hiérarchique plus élevé, l'instauration d'une *Task Force* ou de comités, le recours à des spécialistes externes ou la commande d'expertises externes, l'affectation de ressources plus importantes ou distinctes, etc.

Le Cm 136 a été laissé tel quel. Ce Cm n'a pas vocation à contourner la procédure régulière d'audition ; pour toute nouvelle annexe ou tout nouveau thème, la FINMA appliquera le processus de réglementation alors valable[5]. Si les établissements ou les branches ne devaient pas remplir les exigences d'après le Cm 135, la circulaire serait ponctuellement adaptée en lien avec le Cm 136.

[5] Lignes directrices actuelles applicables à la réglementation des marchés financiers : http://www.finma.ch/f/regulierung/pages/regulierungsprozess.aspx

Conclusion

Le Cm 135 a été remanié. En revanche, toute adaptation du Cm 136 a été abandonnée.

3.2 Traitement des données électroniques de clients (annexe 3)

3.2.1 Critique générale

- Approche fondée sur les seuls principes ou approche détaillée : plusieurs prises de position se sont exprimées sur le degré de précision de l'annexe 3 et ont proposé une «approche fondée sur les seuls principes » plutôt que l'« approche détaillée » choisie dans le cadre de l'audition. Des doutes ont notamment été émis sur la capacité des exigences figurant à l'annexe 3 de permettre une implémentation spécifique à l'établissement (pour ce qui est par ex. des différents systèmes de technologie de l'information ou de la planification de l'organisation). L'argument selon lequel ces exigences pourraient rapidement s'avérer caduques du fait des évolutions techniques a également été avancé.
- Plusieurs prises de position ont également fait état des conséquences en termes de coûts de l'implémentation de ces exigences et ont qualifiées ces dernières de matérielles.

Appréciation

Quelques prises de position ont salué le principe d'une réglementation du traitement des données électroniques de clients. A l'avenir aussi, la confidentialité des données des clients doit se voir accorder, sur la place financière suisse, l'importance qui lui revient. Des places financières comparables ont publié des réglementations en ce sens (UK FSA « Data Security in Financial Services » [avril 2008] ou Singapore MAS « Technology Risk Management Guidelines » [juin 2013]). Par ailleurs, seules quelques prises de position ont proposé l'autorégulation comme alternative. A l'occasion du workshop commun de mars 2013, l'ASB a noté à ce sujet : « Le document " Data Leakage Protection "[6] publié par l'ASB n'[est] pas une recommandation, mais un document informatif qui n'est pas sujet aux travaux de révision ». Ce document présente par conséquent les *Best Practices* qui, par définition, ne sont pas conçues à des fins d'autorégulation et ne peuvent pas être utilisées en ce sens.

Pour le reste, la critique portait sur la granularité des exigences et sur leur niveau réglementaire. La FINMA est d'avis que l'approche choisie est en grande partie fondée sur des principes et non sur des règles. Les exigences posées dans l'annexe 3 ne font qu'un recours marginal à des concepts techniques (s'en tenant à ceux d'anonymisation, de pseudonymisation et de chiffrement) et ne constituent donc pas une entrave à une application spécifique aux établissements. L'approche choisie, fondée sur les principes, garantit la validité temporelle dans la mesure où les évolutions techniques n'exigeront une actualisation de principes s'abstenant de toute formulation technique qu'à long terme.

[6] 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).

Comparées aux exigences qualitatives de base du chapitre IV.B, celles figurant à l'annexe 3 se caractérisent par une granularité spécifique au risque. Afin que l'annexe 3 offre une complémentarité optimale aux exigences qualitatives de base du chapitre IV.B (cf. Cm 135, 136) et puisse être efficace, le traitement des données électroniques de client est plus détaillé à dessein.

Les objections formulées dans les prises de position au sujet du degré de précision des exigences ont été prises en compte ponctuellement et le texte de l'annexe 3 a subi des coupes notables en certains endroits.

Pour ce qui est des coûts d'implémentation des exigences, il est important de faire la distinction entre les établissements qui accusent un retard général au niveau de leur infrastructure informatique de ceux qui ont déjà investi dans une infrastructure informatique solide et qui ont planifié et mobilisé des mesures adéquates pour conserver ce niveau à l'avenir. Que ce soit directement dans le cadre de ses activités de surveillance ou en s'appuyant sur le travail des organes de révision, la FINMA va suivre avec intérêt l'implémentation des exigences et observer quels établissements relèvent de la première ou de la seconde des catégories précitées.

Conclusion

Une réduction drastique du degré de précision aux seuls principes a été rejetée. Le texte de l'annexe 3 a cependant été fortement réduit.

Autre critique

Les prises de position reçues concernaient pour l'essentiel les points suivants :

- Règles, processus et systèmes (Cm 6)
- Définition des CID, classification et exceptions (Cm 9 à 12) ainsi que chapitre III (Cm 67)
- Lieu de stockage et accès aux données depuis l'étranger (Cm 20 à 23)
- Principe du *need to know* (Cm 24 à 26)
- Liste des collaborateurs ayant accès aux CID et liste des « collaborateurs clés » (Cm 28, 29, 41)
- Sélection soigneuse des collaborateurs (Cm 38)
- Environnement de production, opérations portant sur une grande quantité de CID (Cm 47)
- Annonce (Cm 51)

D'autres objections de moindre importance ont été reprises, mais sans donner lieu à un commentaire particulier dans le présent rapport.

3.2.2 Règles, processus et systèmes (Cm 6)

Prises de position (résumées)

- La Chambre fiduciaire attire l'attention sur le fait que les concepts cadres exigés et leur respect ne pourront être contrôlés que si les établissements les concrétisent (pour ce qui est des mesures et de leurs fréquences notamment). La Chambre fiduciaire propose donc de faire un ajout au texte.

Conclusion

La suggestion de la Chambre fiduciaire a été reprise sous la forme d'un nouveau Cm 7.

3.2.3 Définition des CID, classification et exceptions (Cm 9 à 12) ainsi que chapitre III (Cm 67)

Prises de position (résumées)

- Plusieurs prises de position se sont exprimées sur la définition des CID et sur la classification qui en a été faite à titre d'illustration au chapitre III. Par ailleurs, de nombreuses questions ont été posées, par ex. pour savoir si l'implémentation pouvait être différente selon les segments, si les communications aux instances externes (telles que l'encaissement) pouvaient être considérées comme des exceptions à la confidentialité des CID.

Appréciation

Comme en dépit de la formulation du Cm 10 et des explications spécifiques apportées dans le rapport explicatif, il ne ressortait pas clairement que la définition et la classification des CID incombaient à l'établissement, l'exemple du chapitre III et les références correspondantes dans la circulaire ont été supprimés.

Cette mesure répond au souhait général de ne pas voir les exigences afficher un trop haut degré de précision et de granularité. Par conséquent, la conception est entre les mains des établissements.

Conclusion

Les exemples illustrant la définition des CID au chapitre III ainsi que les références correspondantes dans la circulaire ont été supprimés.

3.2.4 Lieu de stockage et accès aux données depuis l'étranger (Cm 20 à 23)

Prises de position (résumées)

- Plusieurs prises de position se sont exprimées sur les réglementations visées aux Cm 20 à 23, jugées inadéquates et trop détaillées, ainsi que sur d'éventuelles incohérences par rapport à la circulaire 2008/7 « Outsourcing – banques ».

- L'ASB précise que « concernant certaines réglementations détaillées, la FINMA va même au-delà des obligations relevant du droit de la protection des données et procède à une " révision de la loi de fait " en menant une audition sur des obligations d'organisation qui ne sont pas prévues par la loi. Il est possible de convoquer ici l'exemple suivant : chiffre marginal 23* : des exigences s'ajoutent à celles prévues par la Circ.-FINMA 08/7 « Outsourcing – banques » pour les transactions externalisées. Les dispositions relatives à l'outsourcing, actuellement définies dans le cadre de la Circ.-FINMA 08/7, ne doivent pas être limitées par les prescriptions de la nouvelle annexe 3, ni alourdies par une charge supplémentaire disproportionnées ».

Appréciation

Les Cm 20 à 23 visent à éliminer les incohérences dans l'implémentation observées entre les établissements et les interprétations divergentes des exigences existantes (dont la Circ.-FINMA 08/07 « Outsourcing – banques » par les organes de révision. Par exemple, il a été constaté que la suppression de l'exigence d'adresser au client une lettre spécifique lors de l'anonymisation[7] de CID qui sont stockées hors de Suisse ou qui sont accessibles depuis l'étranger n'a pas été comprise par tous les établissements.

En vertu de la prise de position écrite du Préposé fédéral à la protection des données et à la transparence (PFPDT), la FINMA est en mesure de déclarer dans le rapport explicatif comme dans le présent document que seules des données anonymisées (au sens de la définition figurant dans le glossaire qui délimite cette notion de celles de pseudonymisation et de chiffrement) ne permettent aucune remontée jusqu'à l'identité du client concerné et que donc l'obligation d'adresser une lettre spécifique au client conformément au Cm 39 de la Circ.-FINMA 08/7 n'est caduque que dans le cas de données anonymisées.

Toutefois, le souhait de ne pas voir les exigences afficher un trop haut degré de précision et de granularité a été pris en compte et les Cm 20 à 23 ont été réduits à un seul paragraphe fondé sur des principes.

Conclusion

Le Cm 20 a été légèrement modifié et les Cm 21 à 23 ont été purement et simplement biffés.

[7] Au sens de la définition figurant dans le glossaire qui délimite cette notion de celles de pseudonymisation et de chiffrement.

3.2.5 Principe du *need to know* (Cm 24 à 26)

Prises de position (résumées)

- L'ASB s'est exprimée comme suit au sujet du Cm 24 : « Les exceptions prévues pour les plus petites banques (Cm 2*) ne sont pas concluantes. La raison pour laquelle un établissement de plus petite taille devrait être exempté du principe du *need to know* (Cm 24*) est par exemple d'autant plus incompréhensible qu'il s'agit d'un principe de base de la protection des données ». La même remarque a aussi été avancée par la BCG.

- Plusieurs prises de position se sont dites défavorables à la précision de la répartition des droits d'accès prévue aux Cm 25 et 26.

Appréciation

Le principe du *need to know* a été résumé à une seule phrase et sera, dans la version finale, applicable à toutes les banques, sans autres précisions. Le Cm 2 a été actualisé en conséquence.

Conclusion

Les Cm 2 et 24 ont été légèrement modifiés et les Cm 25 et 26 ont été purement et simplement biffés.

3.2.6 Liste des collaborateurs ayant accès aux CID et liste des « collaborateurs clés » (Cm 28, 29, 41)

Prises de position (résumées)

- Plusieurs prises de position se montrent sceptiques quant à l'intérêt d'une liste des collaborateurs ayant accès aux CID. A titre d'exemple, la BCG émet le commentaire suivant : « Nous sommes d'avis que ce point confond causes et conséquences. Nous sommes convaincus que les droits d'accès doivent être attribués par un système automatisé, éventuellement en fonction des rôles. La liste recensant tous les droits d'accès s'entend donc une production (un rapport) de ce programme ».

Appréciation

Le Cm 28 a été modifié dans le sens du commentaire de la BCG.

Conclusion

Le Cm 28 a été adapté et la teneur du Cm 29 a été intégrée au Cm 41.

3.2.7 Sélection soigneuse des collaborateurs (Cm 38)

Prises de position (résumées)

- SIX Securities Services a apporté le commentaire suivant : « Une banque ne peut pas garantir les processus de tiers ; une banque peut de préférence et devrait consigner contractuellement ces obligations et se réserver le droit de s'assurer du respect de ces exigences par le biais d'un contrôle ».

Appréciation

Le Cm 38 a été modifié dans le sens du commentaire de SIX Security Services.

Conclusion

Le Cm 38 a été adapté.

3.2.8 Environnement de production, activités en lien avec les CID en masse (Cm 47)

Prises de position (résumées)

- Plusieurs prises de position se sont exprimées sur la notion d'« activités » et ont demandé qu'elle soit précisée.

Appréciation

Le Cm 47 se concentre sur le travail des administrateurs des moyens informatiques et des collaborateurs (y compris des tiers) ayant des droits d'accès supérieurs. Dans ce domaine, le terme « activités » renvoie typiquement au « traitement de données » en lien avec de grandes quantités de CID. Ces « activités » appartenant au profil des tâches des collaborateurs précités, elles ne peuvent n'être ni limitées, ni empêchées. Les mesures de sécurité envisageables s'appuient sur deux aspects :

- la communication de ces activités à l'unité compétente pour la sécurité des données auprès de laquelle elles doivent être déclarées;
- la traçabilité des activités effectuées, soit par des moyens électroniques (comme les fichiers journaux), soit par d'autres mesures (par ex. principe du double contrôle).

Conclusion

Le Cm 47 a été adapté en conséquence.

3.2.9 Objet (Cm 51)

Prises de position (résumées)

- Commentaire de la BCG : « Nous sommes d'avis que les événements qui touchent au CID relèvent du plus haut niveau de confidentialité et ne doivent pas faire l'objet de " rapports classiques ", ni être disséminés dans un rapport spécifique. Il est de l'intérêt de la banque d'apprendre de ses erreurs, mais pas d'expliquer à tout à chacun les mécanismes qui ont rendu possible (ou n'ont pas empêché) un tel événement ». Elle propose une autre formulation.

- Commentaire de SIX Securities Services : « La confidentialité en soi n'est pas un risque ».

Conclusion

Le Cm 51 a été adapté en conséquence.

3.3 Questions spécifiques relatives à l'audition et autres thèmes

Les prises de position reçues concernaient pour l'essentiel les points suivants:

- Questions relatives à l'audition
- Fonds propres minimaux et plancher (*floor* ; Cm 116)

3.3.1 Questions relatives à l'audition

Dans le cadre de cette audition, la FINMA a posé les questions spécifiques suivantes :

1. Chapitre IV.B « Exigences qualitatives de base » :

Dans le projet, l'entrée en vigueur de ce chapitre est prévue pour le 1er janvier 2015.

Comment évalueriez-vous la possibilité d'avancer l'entrée en vigueur du chapitre IV.B « Exigences qualitatives de base » au 1er juillet 2014 ?

(L'annexe 3 « Traitement des données électroniques de clients » entrerait en vigueur au 1er janvier 2015 comme prévu.)

2. Annexe 3 « Traitement des données électroniques de clients » :

Dans le projet, cette annexe concerne uniquement les personnes physiques (« particuliers ») dont les relations commerciales sont suivies ou gérées en Suisse ou depuis la Suisse.

Comment évalueriez-vous la possibilité d'une extension du domaine d'application

a) aux personnes physiques (« particuliers ») dont les relations commerciales sont suivies ou gérées à l'étranger ?

b) aux personnes morales (par ex. « entreprises ») ?

Les réponses reçues concernaient pour l'essentiel les points suivants :

- Pour ce qui est du point 1), toutes les réponses reçues étaient négatives et rejetaient la possibilité d'une entrée en vigueur anticipée au 1er juillet 2014.
- Concernant le point 2a), de nombreuses prises de positions se sont avérées négatives. L'AFBS a souligné que du fait des différences existant dans les réglementations en matière de protection des données et au regard d'autres exigences spécifiques (par ex. celles du Royaume-Uni et de Singapour[8]), il pourrait en résulter des contradictions difficilement gérables ou des doublons. De plus, Credit Suisse a souligné qu'une extension aux relations clientèle suivies ou gérées à l'étranger augmenterait considérablement la complexité en termes de calendriers, de ressources et de coûts.
- Le point 2b) n'a suscité que peu de résistance sur le fonds. Quelques prises de position ont estimé que la possibilité d'une extension du domaine d'application de l'annexe 3 aux personnes morales était faisable puisque des systèmes comparables sont déjà utilisés à l'heure actuelle dans des établissements de moindre taille. Elles insistent cependant aussi sur le fait que les personnes morales ne sont pas la cible de l'annexe 3. C'est dans ce contexte que la Chambre fiduciaire précise : « les particuliers qui n'entretiennent pas des relations commerciales directement avec les banques, mais par l'entremise de sociétés de siège, de sociétés de domicile, de fondations, de trusts ou de toute autre forme juridique ne sont pas considérés comme des « personnes morales ».

Appréciation

La FINMA n'a pas modifié la version soumise à audition au vu des questions spécifiques 1) et 2a), ce qui correspond à la majorité des prises de position reçues.

Une extension aux personnes morales telle qu'elle avait envisagé sous 2b) aurait été possible. La FINMA a décidé pour des aspects liés au rapport coûts/avantages de ne pas réaliser cette extension au domaine d'application selon des modalités prescriptives. L'application des exigences figurant dans l'annexe reste recommandée pour les CID des personnes morales, mais n'est pas considérée comme impérative.

Les objections de la Chambre fiduciaire ont été prises en compte par l'ajout d'une précision au Cm 1.

[8] UK FSA « Data Security in Financial Services » (avril 2008) ou Singapore MAS « Technology Risk Management Guidelines » (juin 2013)

Conclusion

Le volet de la circulaire concernant les exigences qualitatives de base entre lui-aussi en vigueur au 1er janvier 2015. Le domaine d'application de l'annexe 3 demeure inchangé, à l'exception d'une précision du Cm 1.

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

Prises de position (résumées)

- Credit Suisse, UBS et l'ASB ont demandé de plus amples explications sur l'application du Cm 116 aux banques AMA et notamment sur la méthode à utiliser.

Appréciation

Les nouvelles dispositions relatives aux fonds propres minimaux et au plancher harmonisent la Circ.-FINMA 08/21 avec les chiffres marginaux 381 à 381.1 de la circulaire FINMA 2008/19 « Risques de crédit – banques ». Elles ne sont déterminantes que pour les banques qui utilisent l'approche AMA.

Le calcul des fonds propres minimaux pour les risques opérationnels se réfère à l'approche standard selon l'art. 93 de l'ordonnance sur les fonds propres (OFR ; RS 952.03). Cette information est ajoutée au Cm 116.

La FINMA attire l'attention sur le fait que toutes les exigences en fonds propres doivent toujours être prises en compte lors du calcul du *floor*. Pour ce faire, une procédure interne recourant à l'application de l'approche standard intervient à ce stade. Par conséquent, il n'est jamais question d'une comparaison segmentée dans laquelle l'approche standard pour les risques opérationnels est mise en rapport seule avec les exigences de fonds propres selon l'AMA.

Comme dans la plupart des cas, la part des fonds propres requis pour les risques opérationnels est faible par rapport au total des fonds propres requis (elle ne dépasse 40 % que dans certains cas extrêmes), la probabilité que l'application de l'approche AMA entraîne seule une réduction de 20 % au niveau de la banque dans son ensemble reste très faible. Même pour une banque qui est très fortement exposée aux risques opérationnels (à titre d'exemple, on prend pour hypothèse que cette part se monte à 40 % en effectuant le calcul au moyen de l'approche standard – AS – pour les risques opérationnels), il en résulterait une réduction de 20 % de sorte que les exigences en fonds propres pour les risques opérationnels selon l'AMA seraient de 50 % inférieures à celles obtenues en appliquant l'AS. La FINMA ne manquerait pas de porter un jugement très critique sur une telle réduction.

Conclusion

Le Cm 116 a été remanié comme mentionné.

4 Prochaines étapes

La révision partielle de la circulaire « Risques opérationnels – banques » est accueillie très diversement. Comme les principales critiques se sont concentrées sur l'annexe 3 de la circulaire, la FINMA s'est notamment repenchée sur la thématique du « Traitement des données électroniques de clients» en y intégrant une large part des résultats de l'audition.

La révision partielle de la circulaire entre en vigueur au 1er janvier 2015.