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

Circulaire 2008/21
Risques opérationnels – banques

Exigences de fonds propres et exigences qualitatives relatives aux risques opérationnels dans le secteur bancaire

Référence :	Circ.-FINMA 08/21 « Risques opérationnels – banques »
Date :	20 novembre 2008
Entrée en vigueur :	1er janvier 2009
Dernière modification :	XXX ~~1er juin 2012~~ [les modifications sont signalées par * et figurent à la fin du document]
Concordance :	remplace la Circ.-CFB 06/3 « Risques opérationnels » du 29 septembre 2006
Bases légales :	LFINMA art. 7 al. 1 let. b
	LB art. 3 al. 2 let. a et b, 3g, 4 al. 2 et 4, 4bis al. 2
	OB art. 9 al. 2 et 4
	LBVM art. 10 al. 2 let. a
	OBVM art. 19 al. 3, 20 al. 1, 29
	OFR art. 2, 89–94
	Oém-FINMA art. 5 ss
~~Annexe 1 :~~	~~Exigences qualitatives de base~~
Annexe ~~2~~1:	Classification des segments d'affaires pour la classification conformément à l'art. 93 al. 2 OFR
Annexe ~~3~~2 :	Vue d'ensemble pour la classfication des types d'événements
Annexe ~~4~~3 :	~~Comparaison entre la Circ. FINMA et les standards minimaux du Comité de Bâle~~ Traitement des données électroniques de clients

Einsteinstrasse 2, 3003 Berne
Tél. +41 (0)31 327 9100, Fax +41 (0)31 327 9101
www.finma.ch

x	Banques	LB	Destinataires
x	Groupes et congl. financiers		
	Autres intermédiaires		
	Assureurs	LSA	
	Groupes. et congl. d'assur.		
	Intermédiaires d'assur.		
	Bourses et participants	LBVM	
x	Négociants en valeurs mob.		
	Directions de fonds	LPCC	
	SICAV		
	Sociétés en comm. de PCC		
	SICAF		
	Banques dépositaires		
	Gestionnaires de PCC		
	Distributeurs		
	Représentants de PCC étr.		
	Autres intermédiaires		
	OAR	LBA	
	IFDS		
	Entités surveillées par OAR		
	Sociétés d'audit	Autres	
	Agences de notation		

Table des matières

Table des matières

I. Objet

1*

La présente Circulaire concrétise les art. 89–94 de l'ordonnance sur les fonds propres (OFR ; RS 952.03) et définit les exigences qualitatives de base pour la gestion des risques opérationnels en vertu de l'art. 9 OB et de l'art. 19 s OBVM. Dans le domaine quantitatif, ~~E~~elle régit le calcul des exigences de fonds propres relatives aux risques opérationnels en fonction des trois approches à disposition ainsi que les obligations qui en découlent. Les exigences qualitatives de base correspondent aux recommandations du Comité de Bâle pour une gestion irréprochable des risques opérationnels.

II. Définition ~~(art. 92 OFR)~~

2

En vertu de l'art. 89 OFR, les risques opérationnels sont définis comme étant «le risque de pertes provenant de l'inadéquation ou de la défaillance de procédures internes, de personnes, de systèmes ou suite à des événements externes». Cette définition inclut l'ensemble des risques juridiques, y compris les amendes d'autorités de surveillance et les arrangements. Elle exclut toutefois les risques stratégiques et de réputation.

2.1*

Conformément à l'art. 89 OFR, les risques de réputation sont exclus de la définition des risques opérationnels, dans la mesure où ils sont, en règle générale, difficiles, voire impossibles à quantifier. Il convient néanmoins de souligner que la réalisation de risques opérationnels peut avoir des répercussions indirectes et potentiellement graves sur la réputation d'une banque.

III. Exigences de fonds propres

A. L'approche de l'indicateur de base (BIA, art. 92 OFR)~~(BIA, art. 80 OFR)~~

3

Pour les banques qui utilisent l'approche de l'indicateur de base pour calculer leurs exigences de fonds propres au titre des risques opérationnels, celles-ci équivalent au produit du multiplicateur α et de la moyenne tirée des trois dernières années écoulées de l'indicateur des revenus annuels (GI)[1]. Cependant, seules les années durant lesquelles le GI affiche une valeur positive sont prises en compte pour le calcul de la moyenne.

4

Les trois dernières années écoulées au sens du Cm 3 (ainsi que du Cm 24) correspondent aux trois périodes qui précèdent directement la date d'établissement du dernier compte de ré-

[1] Dans la version révisée des standards minimaux du Comité de Bâle sur le contrôle bancaire (« *International Convergence of Capital Measurement and Capital Standards – A Revised Framework / Comprehensive Version* ») de juin 2006, l'indicateur des revenus est désigné par «Gross Income» (GI).

sultat publié. Par exemple, si le dernier compte de résultat publié se rapporte à la date du 30 juin 2008, les trois années à prendre en compte correspondent ainsi aux périodes du 1er juillet 2005 au 30 juin 2006, 1er juillet 2006 au 30 juin 2007 et 1er juillet 2007 au 30 juin 2008.

Les exigences de fonds propres K_{BIA} sont ainsi obtenues comme suit : 5

$$K_{BIA} = \alpha \cdot \sum_{j=1}^{3} \frac{\max[0, GI_j]}{\max[1, n]}$$

où

- α est fixé uniformément à 15 %; 6
- GI_j correspond à l'indicateur des revenus de l'année j; et 7
- n représente le nombre d'années pour lesquelles un indicateur des revenus GI positif a été enregistré sur les trois années écoulées. 8

L'indicateur des revenus GI correspond à la somme des positions suivantes du compte de résultat, conformément aux Cm 103 ss Circ.-FINMA 08/2 « Comptabilité – banques » : 9

- résultat des opérations d'intérêts (Cm 105–109 Circ.-FINMA 08/2 « Comptabilité – banques »); 10
- résultat des opérations de commissions et des prestations de service[2] (Cm 110–116 Circ.-FINMA 08/2 « Comptabilité – banques »); 11
- résultat des opérations de négoce (Cm 117 Circ.-FINMA 08/2 « Comptabilité – banques »); 12
- résultat des participations non consolidées (Cm 119 s Circ.-FINMA 08/2 « Comptabilité – banques »); et 13
- résultat des immeubles (Cm 121 s Circ.-FINMA 08/2 « Comptabilité – banques »). 14

La base de calcul au niveau consolidé de l'indicateur des revenus GI correspond au cercle de consolidation relatif à la détermination des exigences de fonds propres. 15

Lorsque la structure ou les activités d'une banque sont élargies (par exemple suite à la reprise d'une nouvelle unité d'affaires), les valeurs historique de l'indicateur des revenus GI sont adaptées en conséquence vers le haut. Les réductions de l'indicateur des revenus GI (par exemple suite à l'aliénation d'une unité d'affaires) sont subordonnées à une autorisation de l'a FINMA. 16

[2] La prise en considération des charges de commissions selon le Cm 114 Circ.-FINMA 08/2 « Comptabilité – banques » est soumise aux restrictions du Cm 18.

Les banques peuvent déterminer l'indicateur des revenus GI selon l'art. 91 al. 1 OFR sur la base des prescriptions internationales d'établissement des comptes reconnues en lieu et place des prescriptions suisses régissant l'établissement des comptes, dans la mesure où la FINMA octroie une autorisation correspondante (cf. art. 91 al. 4 OFR). 17

Tous les produits provenant d'accords d'externalisation («outsourcing») suivant lesquels la banque fournit des prestations à des tiers doivent être inclus dans l'indicateur des revenus GI (cf. art. 91 al. 2 OFR). 18

Lorsqu'une banque apparaît au titre de mandantes de services externalisés, elle ne peut déduire les charges correspondantes de l'indicateur des revenus GI que si l'externalisation est effectuée au sein du même groupe financier et qu'elle est englobée dans la consolidation (cf. art. 91 al. 3 OFR). 19

~~Les banques qui appliquent l'approche de l'indicateur de base doivent satisfaire aux exigences qualitatives de base décrites dans l'annexe 1 si~~ Abrogé 20*

- ~~leurs exigences de fonds propres KBIA ont dépassé au moins une fois le montant de 100 millions de CHF au cours des trois dernières années écoulées; ou si~~ Abrogé 21*
- ~~elles sont représentées à l'étranger par des succursales ou des sociétés du groupe devant être consolidées en vertu des dispositions relatives aux fonds propres et qui représentent de manière agrégée plus de 5 % des fonds propres exigibles pour les risques opérationnels.~~ Abrogé 22*

B. L'approche standard (SA ; art. 93 OFR)

a) Mécanisme

Pour déterminer les exigences de fonds propres, les banques doivent répartir l'ensemble de leurs activités sur les segments d'affaires ci-après : 23

i	Segment d'affaires	β_i
1	Financement et conseil d'entreprises	18%
2	Négoce	18%
3	Affaires de la clientèle privée	12%
4	Affaires de la clientèle commerciale	15%
5	Trafic des paiements / règlement de titres	18%
6	Affaires de dépôt et dépôts fiduciaires	15%
7	Gestion de fortune institutionnelle	12%
8	Opérations de commissions sur titres	12%

Tableau 1

Un indicateur des revenus est calculé, selon les Cm 9–18, pour chaque segment d'affaires i et pour chacune des trois années écoulées selon le Cm 4, puis multiplié par le facteur β_i indiqué dans le tableau 1. Les valeurs ainsi obtenues sont additionnées afin d'obtenir des sommes annuelles; lorsque des segments spécifiques affichent des valeurs négatives, celles-ci peuvent être compensées avec les valeurs positives d'autres segments. Les 24

exigences de fonds propres correspondent au montant moyen sur trois ans. Les montants négatifs éventuels sont cependant mis à zéro lors de la détermination de la moyenne (cf. art. 93 al. 1 OFR).

Dans l'approche standard K_{SA}, les exigences de fonds propres sont la résultante de 25

$$K_{SA} = \frac{1}{3} \cdot \sum_{j=1}^{3} \max\left[0, \sum_{i=1}^{8} GI_{i,j} \cdot \beta_i\right]$$

En l'occurrence,

- $GI_{i,j}$ correspond à l'indicateur de revenus GI pour un segment d'affaires donné pendant l'année déterminante j, et 26
- β_i correspond à un pourcentage fixe donné, identique pour toutes les banques, pour un segment d'affaires donné. 27

b) Exigences générales (art. 93 al. 3 OFR)

~~Toutes les banques qui appliquent l'approche standard doivent satisfaire aux exigences qualitatives de base figurant dans l'annexe 1.~~ Abrogé 28*

Chaque banque doit définir, conformément à l'annexe ~~2~~1, des principes spécifiques pour la répartition de ses activités dans les segments d'affaires standardisés selon le Cm 23 et disposer à cet effet de critères consignés par écrit. Ces critères doivent être régulièrement vérifiés et adaptés en fonction des changements intervenant dans les activités de la banque. 29*

c) ~~Exigences supplémentaires pour les banques actives à l'étranger~~Abrogé

~~Une banque qui dispose à l'étranger de succursales ou de sociétés du groupe devant être consolidées selon les dispositions relatives aux fonds propres doit satisfaire en plus aux exigences définies aux Cm 31–44.~~ Abrogé 30*

~~La banque doit disposer d'un service chargé de la gestion des risques opérationnels, qui assume la responsabilité~~ Abrogé 31*

- ~~du développement de stratégies pour l'identification, l'analyse, la surveillance, le contrôle et l'atténuation des risques opérationnels;~~ Abrogé 32*
- ~~de l'établissement de principes et de procédures valables dans l'ensemble de la banque pour la gestion et le contrôle des risques opérationnels;~~ Abrogé 33*
- ~~de la conception et de la mise en œuvre d'une méthodologie pour l'analyse des risques opérationnels; et~~ Abrogé 34*
- ~~de la conception et de la mise en œuvre d'un système d'annonce des risques opérationnels.~~ Abrogé 35*

~~Dans le cadre du système interne d'analyse des risques opérationnels, la banque doit collecter systématiquement les données pertinentes y relatives, y compris les pertes significatives survenues dans les différents segments d'affaires.~~ Abrogé

36*

~~Le système d'analyse doit être étroitement intégré dans les processus de gestion des risques de la banque.~~ Abrogé

37*

~~Les enseignements obtenus par ce biais doivent faire partie intégrante des processus de surveillance et de contrôle du profil de risque opérationnel propre à l'établissement. Ces informations doivent par exemple jouer un rôle prédominant dans les rapports remis au « management » et dans l'analyse des risques.~~ Abrogé

38*

~~La banque doit disposer de systèmes incitatifs à même de contribuer à l'amélioration de la gestion des risques opérationnels.~~ Abrogé

39*

~~Les responsables des différents segments d'affaires, la direction générale ainsi que l'organe exerçant la haute direction, la surveillance et le contrôle doivent être informés régulièrement de l'exposition aux risques opérationnels ainsi que des événements générateurs de pertes opérationnelles significatives. La banque doit disposer de procédures lui permettant de réagir adéquatement à de telles informations.~~ Abrogé

40*

~~Le système de gestion des risques opérationnels de la banque doit être bien documenté.~~ Abrogé

41*

~~La banque doit disposer de procédures garantissant le respect des principes, contrôles et procédures internes consignés par écrit relatifs au système de gestion des risques opérationnels. La définition de principes pour la gestion des infractions internes en fait également partie.~~ Abrogé

42*

~~Les processus de gestion des risques opérationnels dans la banque et le système d'analyse correspondant doivent faire régulièrement l'objet d'une validation et d'une vérification indépendantes. Ces contrôles doivent porter à la fois sur les activités des différents segments d'affaires et sur la fonction de gestion des risques opérationnels.~~ Abrogé

43*

~~Le système d'analyse des risques opérationnels de la banque (y compris les processus de validation internes) doit régulièrement faire l'objet de vérifications par la société d'audit.~~ Abrogé

44*

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

a) Autorisation

Les approches spécifiques aux établissements («Advanced Measurement Approaches», AMA), permettent aux banques de quantifier elles-mêmes, en respectant certaines conditions, leurs exigences de fonds propres relatives aux risques opérationnels en appliquant une procédure individuelle.

45

Le recours à une approche spécifique à l'établissement nécessite une autorisation de la

46

FINMA.

47 Avant d'octroyer une autorisation pour l'utilisation d'une approche spécifique à l'établissement, la FINMA peut exiger des banques qu'elles effectuent sur une période de deux ans au maximum, à des fins de test et de comparaison, des calculs fondés sur l'approche en question.

48 Une banque qui applique une approche spécifique à l'établissement ne peut passer entièrement ou partiellement à l'approche de l'indicateur de base ou à l'approche standard que sur injonction ou avec l'autorisation de la FINMA.

49 Les charges occasionnées à la FINMA par la procédure d'autorisation et par les travaux de vérification nécessaires après l'octroi de l'autorisation sont facturées aux banques concernées.

b) Exigences qualitatives supplémentaires

50* Les banques qui utilisent une approche spécifique à l'établissement doivent satisfaire aux exigences qualitatives de base selon ~~l'annexe 1~~ le chapitre IV.B.

51 Afin de pouvoir utiliser une approche spécifique à l'établissement pour le calcul des exigences de fonds propres relatives aux risques opérationnels, il est en plus nécessaire de satisfaire aux autres exigences qualitatives mentionnées ci-après.

52 L'organe exerçant la haute direction, la surveillance et le contrôle doit être impliqué de manière active dans la surveillance de l'approche.

53* La ~~gestion des affaires~~ direction opérationnelle doit être familiarisée avec le concept de base de l'approche et être à même d'exercer ses fonctions de surveillance en la matière.

54 La banque dispose pour la gestion des risques opérationnels d'un système conceptionnel solidement conçu, fiable et mis en œuvre avec intégrité.

55 A tous les niveaux de la banque, des ressources suffisantes sont disponibles pour les activités de gestion, de contrôle et de révision interne en rapport avec l'approche spécifique à l'établissement.

56 La banque doit disposer d'une unité centrale indépendante de gestion des risques opérationnels, qui assume la responsabilité de l'élaboration et de la mise en œuvre des principes régissant la gestion des risques opérationnels. Cette unité est compétente pour :

- 57 l'établissement de principes et de procédures pour la gestion et le contrôle des risques opérationnels à l'échelle de la banque;
- 58 la conception et l'application de la méthodologie de quantification des risques opérationnels propre à l'établissement;

- la conception et la mise en place d'un système d'annonce des risques opérationnels; et

59

- le développement de stratégies pour l'identification, la mesure, la surveillance ainsi que le contrôle et l'atténuation des risques opérationnels.

60

Le système de quantification propre à l'établissement doit être étroitement intégré dans les processus de gestion quotidienne des risques de la banque.

61

Les résultats du système de quantification propre à l'établissement doivent faire partie intégrante de la surveillance et du contrôle du profil de risque. Ces informations doivent par exemple jouer un rôle important dans les rapports remis au « management », dans l'allocation interne des fonds propres et dans l'analyse des risques.

62

La banque doit disposer de méthodes pour l'allocation de fonds propres relatifs aux risques opérationnels dans les segments d'affaires importants et pour la création de systèmes incitatifs à même de contribuer à l'amélioration de la gestion des risques opérationnels dans l'ensemble de la banque.

63

~~Les exigences décrites aux Cm 40–42 doivent être satisfaites afin que l'information et la documentation internes de l'établissement soient assurées.~~ Abrogé

64*

La révision interne et la société d'audit doivent examiner régulièrement les processus de gestion des risques opérationnels et la mise en œuvre de l'approche spécifique à l'établissement. Ces vérifications doivent inclure aussi bien les activités des différentes unités d'affaires que celles de l'unité centrale de gestion des risques opérationnels.

65

La validation du système de quantification par la société d'audit doit en particulier contenir les éléments suivants :

66

- vérification du bon fonctionnement des processuss internes de validation; et

67

- garantie de la transparence et de l'accessibilité des flux de données et processus de l'approche spécifique à l'établissement. Il convient en particulier de s'assurer que la révision interne, la société d'audit et la FINMA puissent accéder aux spécifications et paramètres de l'approche.

68

c) Exigences quantitatives générales

Conformément aux standards minimaux[3] du Comité de Bâle, la FINMA ne spécifie aucune approche déterminée, mais laisse aux banques une grande marge de manœuvre en la matière. Partant, la présente Circulaire se borne à décrire les exigences essentielles qui doivent être impérativement satisfaites pour qu'une telle approche puisse être appliquée. L'examen des spécifications détaillées d'une approche spécifique à l'établissement fait l'objet du processus d'autorisation individuel. Celui-ci a lieu sous la direction de la FINMA, en collaboration

69

[3] Voir note 1.

avec la société d'audit.

70 Indépendamment de la conception concrète de son approche, la banque doit être en mesure de prouver que celle-ci tient également compte des événements susceptibles d'engendrer des pertes significatives mais dont la probabilité de survenance est faible. Les exigences de fonds propres résultant de cette approche doivent correspondre environ au quantile 99,9 % de la fonction de distribution des pertes opérationnelles agrégées sur une année.

71* Chaque approche spécifique à l'établissement doit être fondée sur une notion du risque opérationnel compatible avec la définition de l'art. 89 OFR ainsi qu'au Cm 2. Elle doit en outre permettre de classifier les événements générateurs de pertes conformément à l'annexe ~~3~~2.

72 Des fonds propres exigibles sont déterminées tant pour les pertes attendues qu'inattendues. La FINMA peut toutefois accorder des allégements à cet égard si la banque a constitué des provisions adéquates pour pertes futures attendues.

73 L'ensemble des hypothèses implicites et explicites concernant les rapports entre les événements générateurs de pertes et entre les fonctions d'estimation utilisées doivent être plausibles et justifiées.

74 Chaque approche doit présenter certaines caractéristiques de base. A leur nombre figure notamment la satisfaction des exigences relatives à l'intégration :

- de données internes relatives aux pertes (Cm 76–85);
- de données externes pertinentes relatives aux pertes (Cm 86–88);
- de procédures d'analyses des scénarios (Cm 89–91); et
- de facteurs de l'environnement d'affaires et du système de contrôle interne (Cm 92–97).

75 La banque doit disposer d'un concept fiable, transparent, bien documenté et vérifiable pour la prise en compte et la détermination de l'importance relative de ces quatre éléments fondamentaux dans son approche. Celle-ci doit être cohérente sur le plan interne et éviter en particulier que des éléments atténuant le risque (par exemple des facteurs en rapport avec l'environnement opérationnel et le système de contrôle interne ou des contrats d'assurance) soient pris en compte plusieurs fois.

d) Données internes relatives aux pertes (art. 94 al. 2 OFR)

76 La banque doit disposer de procédures consignées par écrit pour l'évaluation de la pertinence continue des données historiques relatives aux pertes. Celles-ci incluent en particulier des règles internes claires quant à la façon dont la prise en compte des données relatives aux pertes peut être modifiée (par exemple aucune prise en compte en raison de l'absence actuelle de pertinence, mise en échelle en raison de la modification des ordres de grandeur ou toute autre forme d'ajustement). Il convient également de déterminer qui est autorisé à procéder à de telles modifications, et dans quelle mesure.

77 La banque doit utiliser une base de données contenant des données internes relatives aux pertes. Lors de sa première utilisation à des fins réglementaires, celle-ci doit couvrir une pé-

riode d'observation d'au moins trois ans. Deux ans au plus tard après la première utilisation de l'approche, la période d'observation doit s'étendre durablement sur cinq ans au minimum.

78 Le processus de création d'une base de données interne pour les pertes opérationnelles doit satisfaire aux exigences suivantes :

79* • Afin de faciliter la validation par l'autorité de surveillance, la banque doit être en mesure de répartir l'ensemble des données internes relatives aux pertes sur les segments d'affaires indiqués sous le Cm 23 et sur les types d'événements décrits dans l'annexe ~~3~~2. Pour pouvoir procéder à cette classification, elle doit disposer de critères objectifs bien documentés.

80 • Les données internes relatives aux pertes de la banque doivent être collectées dans leur intégralité sur la base d'un processus solide et intègre. Elles doivent couvrir toutes les activités et expositions matérielles, y compris l'ensemble des sous-systèmes et implantations géographiques déterminants. Lors de la collecte des données relatives aux pertes, il est possible de renoncer au recensement systématique des pertes inférieures à un montant minimal brut fixé par la FINMA.

81 • Pour chaque événement générateur de perte, la banque doit collecter les informations suivantes : montant brut de la perte, date de l'événement et atténuations éventuelles de la perte (par exemple du fait de contrats d'assurance). Pour les événements générateurs de perte égaux ou supérieurs à un montant brut de 1 million de CHF, des explications relatives à la cause de la perte doivent être consignées.

82 • La banque doit définir des principes pour la saisie des événements générateurs de pertes. Ceux-ci incluent également des critères pour la classification des événements générateurs de pertes liés à des fonctions centralisées (par exemple service informatique) ou concernant plusieurs segments d'affaires. Par ailleurs, la manière de gérer les successions d'événements générateurs de pertes qui ne sont pas indépendants les uns des autres doit être réglée.

83 Les pertes dues aux risques opérationnels survenues dans le contexte des risques de crédit et prises en compte jusqu'ici comme un risque de crédit peuvent continuer d'être considérées exclusivement, pour le calcul des fonds propres exigibles, comme un événement associé au risque de crédit. A partir d'un certain montant brut fixé par la FINMA, ces pertes doivent être néanmoins intégrées dans la base de données interne relative aux pertes résultant des risques opérationnels et prises en compte pour la gestion de ces derniers. De tels événements générateurs de pertes sont saisis de la même façon que les autres données internes relatives aux pertes, mais ils sont signalés comme n'étant pas pertinents, du point de vue des fonds propres, pour ce qui est des risques opérationnels.

84* Lorsqu'une perte due à un risque opérationnel s'exprime aussi sous la forme d'une perte liée au risque de marché, l'événement correspondant sera traité de la même manière que les autres événements générateurs de pertes et intégré dans l'approche spécifique à l'établissement. Si une banque utilise, conformément aux Cm 228–365 de la Circ.-FINMA 08/20 « Risques de marché – banques », un modèle d'agrégation des risques pour calculer

ses fonds propres exigibles en regard du risque de marché, les positions découlant d'événements liés aux risques opérationnels ne peuvent être exclues ni du calcul du montant exposé au risque (*Value-at-Risk* ou VaR), de la VaR basée sur une simulation de crise, de l'exigence de fonds propres incrémentale (*incremental risk charge*), de la *comprehensive risk measure*, ni du contrôle à posteriori (*backtesting*).

85 Dans le contexte de l'approche spécifique à l'établissement, les éventuelles *«pertes négatives»* (par exemple gains sur une position en actions acquise par erreur) ne doivent pas avoir pour effet de réduire les fonds propres exigibles.

e) Données externes relatives aux pertes (art. 94 al. 2 OFR)

86 Les banques doivent intégrer dans leur approche spécifique des données externes pertinentes relatives aux pertes, ce afin d'assurer la prise en compte d'événements générateurs de pertes peu fréquents mais potentiellement graves. Les données externes publiquement accessibles peuvent servir de source d'informations pertinente, tout comme celles échangées entre certaines banques.

87 Seront pris en compte, dans ces données externes relatives aux pertes, le montant effectif de la perte, des informations quant à l'étendue des activités dans le segment touché par cette dernière, des informations sur les causes et les circonstances de la perte ainsi que des informations concernant l'évaluation de la portée de l'événement générateur de la perte pour la banque elle-même.

88 Les banques doivent définir l'utilisation de données externes relatives aux pertes dans un processus systématique consigné par écrit. Celui-ci doit inclure notamment une méthodologie claire pour l'intégration de ces données dans l'approche spécifique à l'établissement (par exemple mise en échelle, adaptations qualitatives ou influence sur l'analyse de scénarios). Les conditions cadres et les procédures pour l'utilisation de données externes relatives aux pertes sont réexaminées régulièrement tant en interne que par la société d'audit.

f) Analyse de scénarios (art. 94 al. 2 OFR)

89 Les approches spécifiques aux établissements doivent prendre en compte les résultats des analyses de scénarios.

90 Les analyses de scénarios sont basées sur des avis d'experts et des données externes et elles portent sur la crainte que la banque puisse être affectée par des événements générateurs de pertes potentiellement graves.

91 L'actualité et la pertinence des cas de figure retenus pour les analyses de scénarios, de même que les paramètres qui leur sont attribués, sont réexaminés et éventuellement adaptés lors de changements significatifs de la situation en matière de risque, mais au moins une fois par an. En cas de changements significatifs de la situation des risques, les adaptations doivent être effectuées immédiatement.

g) Environnement d'affaires et système de contrôle interne (art. 94 al. 2 OFR)

92 La banque doit prendre en compte à titre prospectif, dans l'approche spécifique à l'établissement, des facteurs prédictifs découlant de l'environnement dans lequel s'exercent ses activités et de son système de contrôle interne. Ceux-ci ont pour but la prise en compte spécifique de caractéristiques actuelles du profil de risque de la banque (par exemple nouvelles activités, nouvelles solutions informatiques, procédures modifiées) ou de changements intervenus dans son environnement (par exemple situation en matière de politique de sécurité, modification de la jurisprudence, menace émanant de virus informatiques).

93 Pour pouvoir être utilisé dans le cadre d'une approche spécifique à l'établissement, les facteurs relatifs à l'environnement opérationnel et au système de contrôle interne doivent satisfaire aux exigences suivantes :

- 94 Chaque facteur doit être un générateur de risque significatif en vertu des expériences faites et de l'appréciation émise par le segment d'affaires concerné. Le facteur sera de préférence quantifiable et vérifiable.

- 95 La sensibilité des estimations de la banque, en matière de risque, aux modifications des facteurs et de leur importance relative doit pouvoir être justifiée et vérifiée. Outre la possibilité d'une modification du profil de risque liée à des améliorations de l'environnement de contrôle, le concept doit notamment prendre en compte des augmentations potentielles des risques dues à une complexité croissante ou à la croissance des activités d'affaires.

- 96 Le concept à proprement parler, de même que le choix et l'utilisation des différents facteurs, y compris les principes fondamentaux régissant l'ajustement des estimations empiriques, doivent être consignés par écrit. La documentation doit également faire l'objet d'une vérification indépendante au sein de la banque.

- 97 Les processus, leurs résultats et les ajustements effectués sont comparés à intervalles réguliers aux expériences effectivement faites, en matière de pertes, tant sur le plan interne qu'externe.

h) Atténuation du risque par des assurances

98 Lorsqu'elles utilisent une approche spécifique (AMA), les banques peuvent tenir compte, lors du calcul de leurs besoins de fonds propres en regard des risques opérationnels, de l'effet d'atténuation du risque produit par des contrats d'assurance. Cependant, la prise en compte de tels effets de couverture est limitée à 20 % au maximum des exigences de fonds propres calculées sur la base d'une approche spécifique à l'établissement.

99 Les possibilités de réduire les exigences de fonds propres sont liées au respect des conditions suivantes :

- 100 L'assureur bénéficie d'une notation de crédit à long terme de la classe de notation 3 ou plus élevée. La notation de crédit doit provenir d'une agence de notation reconnue par

la FINMA.

- Le contrat d'assurance doit porter sur une durée initiale d'au moins un an. Lorsque sa durée résiduelle tombe au-dessous d'une année, la prise en compte de l'effet de couverture sera réduite de façon linéaire de 100 % (pour une durée résiduelle d'au moins 365 jours) à 0 % (pour une durée résiduelle de 90 jours). L'effet de couverture découlant de contrats d'assurance d'une durée résiduelle de 90 jours ou moins n'est pas pris en compte dans le calcul des exigences de fonds propres. 101

- Le contrat d'assurance prévoit un délai de résiliation d'au moins 90 jours. Si le délai de résiliation est inférieur à une année, la prise en compte de l'effet de couverture diminue de façon linéaire, de 100 % (pour un délai de résiliation d'au moins 365 jours) à 0 % (pour un délai de résiliation de 90 jours). Le cas échéant, ces pourcentages seront également appliqués aux effets de couverture déjà réduits en vertu du Cm 101. 102

- Le contrat d'assurance ne doit contenir aucune clause restrictive ou d'exclusion pouvant entraîner, en cas d'intervention de l'autorité de régulation ou d'insolvabilité de la banque concernée, la non-indemnisation de la banque, de son éventuel acquéreur, de la personne chargée de l'assainissement ou du liquidateur. De telles clauses restrictives ou d'exclusion sont cependant admissibles si elles se limitent exclusivement aux événements qui pourraient survenir après l'ouverture de la faillite ou après la liquidation. 103

- L'effet de couverture résultant de contrats d'assurance doit être calculé de façon transparente. Il doit être cohérent en regard de la probabilité utilisée dans l'approche spécifique à l'établissement et de l'ampleur d'un événement générateur de perte potentiel. 104

- Le donneur d'assurance doit être un prestataire externe et ne peut pas appartenir au même groupe que la banque. Dans le cas contraire, les effets de couverture résultant des contrats d'assurance ne peuvent être pris en compte que si le donneur d'assurance reporte les risques sur un tiers indépendant (par exemple une société de réassurance). Pour que l'effet de couverture puisse être pris en compte, ce tiers indépendant doit satisfaire lui-même à l'ensemble des exigences fixées à un donneur d'assurance. 105

- Le concept interne de la banque pour la prise en compte de solutions d'assurance doit être axé sur le transfert effectif des risques. Il doit être bien documenté. 106

- La banque doit publier des informations sur le recours à des solutions d'assurance aux fins d'atténuer les risques opérationnels. 107

D. Utilisation partielle d'approches

Il est en principe possible de limiter à certains domaines d'activité l'utilisation d'une approche spécifique à l'établissement et d'appliquer aux autres soit l'approche de l'indicateur de base, soit l'approche standard. Pour cela, il est nécessaire que les conditions ci-après soient remplies: 108

- Tous les risques opérationnels de la banque sont couverts par une approche mentionnée dans cette Circulaire. Les exigences fixées pour ces approches respectives doivent être satisfaites dans les domaines d'activité correspondants. 109

- Dès qu'une approche spécifique à l'établissement est utilisée, celle-ci doit couvrir une part significative des risques opérationnels de la banque. 110

- La banque doit disposer d'un calendrier fixant le déroulement dans le temps de l'extension de l'approche spécifique à l'établissement à l'ensemble de ses entités juridiques et segments d'affaires matériels. 111

- Il n'est pas permis de conserver l'approche de l'indicateur de base ou l'approche standard dans certains segments d'affaires matériels afin de minorer les exigences de fonds propres. 112

La délimitation entre l'approche spécifique à l'établissement et l'approche de l'indicateur de base ou l'approche standard peut être basée sur des champs d'activité, des structures juridiques, des délimitations géographiques ou d'autres critères distinctifs clairement définis sur le plan interne. 113

Abstraction faite des cas évoqués aux Cm 108–113, il n'est pas permis de recourir à différentes approches pour calculer les besoins en fonds propres d'une banque au titre des risques opérationnels. 114

E. Ajustements des exigences de fonds propres (art. 45 al. 3 OFR)

Dans le cadre de ses fonctions de surveillance concernant des fonds propres additionnels (art. 45 OFR), la FINMA peut majorer individuellement les exigences de fonds propres de certaines banques. De tels relèvements individuels s'imposent en particulier s'il apparait que le calcul des exigences de fonds propres fondé exclusivement sur l'approche de l'indicateur de base ou sur l'approche standard se traduit, en raison d'indicateurs des revenus GI trop faibles, par des exigences de fonds propres réduites et inadéquates. 115

F. Fonds propres minimaux et plancher *(floor)*

Le principe applicable en vertu du maintien du « régime de floor » publié par le Comité de Bâle[4] : pour les banques qui couvrent les risques opérationnels selon l'approche AMA, les exigences minimales en matière de fonds propres à l'échelle de la banque doivent, en considérant également les déductions des fonds propres pouvant être pris en compte, au moins égaler 80 % des exigences et déductions qui auraient été prévues en théorie pour la banque selon le standard minimum de Bâle I.[5] Dans le cas de certains établissements spécifiques, la FINMA règle, en application de l'art. 47 OFR, la manière de procéder au calcul approximatif 116*

[4] Cf. le communiqué de presse du Comité de Bâle daté du 13 juillet 2009 : http://www.bis.org/press/p090713.htm.

[5] Cela correspondrait au calcul des exigences de fonds propres selon l'ordonnance du 17 mai 1972 sur les banques, valable jusqu'au 31 décembre 2006 (RO 1995 253, 1998 16).

adéquat des exigences théoriques selon Bâle I.

IV. Exigences qualitatives

A. Principe de proportionnalité

117* Les exigences du quatrième chapitre de la présente circulaire doivent être mises en œuvre en tenant compte de la taille de la banque. Le Cm 119 recense les chiffres marginaux de l'application desquels les petites banques sont exemptées.

118* Les petites banques au sens du Cm 117 sont :

- les banques appartenant à la catégorie[6] 5 de la FINMA ;
- les négociants en valeurs mobilières des catégories 4 et 5 de la FINMA ;
- ainsi que, dans certains cas, les banques de la catégorie 4 de la FINMA dont les activités d'affaires n'ont pas une complexité significative.

B. Exigences qualitatives de base

119* Les petites banques au sens des Cm 117 et 118 sont exemptées de l'application des Cm 124, 125, 127 let. c à let. i, 128, 130, 131 et 132. Les exigences qualitatives de base reposent sur les « Principles for the Sound Management of Operational Risk » du Comité de Bâle sur le contrôle bancaire (juin 2011).

a) Principe 1 : responsabilités

120* L'organe exerçant la haute direction, la surveillance et le contrôle (ci-après « conseil d'administration ») doit approuver un concept cadre pour la gestion des risques opérationnels, notamment pour définir la propension et la tolérance au risque, et le vérifier régulièrement. Il convient d'y consigner la nature, le type et le niveau des risques opérationnels auxquels la banque est exposée et ceux qu'elle est prête à prendre.

121* La direction opérationnelle doit développer ce concept cadre, le transposer en règles et processus concrets, puis le mettre en œuvre dans les processus de gestion des risques au sein des unités d'affaires, avec instauration de contrôles. Il convient de prévoir des mesures permettant d'identifier à temps les violations de la propension et de la tolérance au risque et d'y remédier.

122* La direction opérationnelle définit une structure de gestion claire, efficace et solide qui assume la responsabilité de la gestion des risques opérationnels. Cette fonction est compétente pour le maintien et le développement permanent du concept cadre pour la gestion des risques opérationnels. Elle doit par ailleurs être pourvue de suffisamment de personnel qualifié pour

[6] Cf. l'annexe de la Circ.-FINMA 11/2 « Volant de fonds propres et planification des fonds propres dans le secteur bancaire ».

pouvoir assumer efficacement ses nombreuses responsabilités. A l'instar des autres fonctions de gestion des risques, la fonction de gestion des risques opérationnels doit bénéficier d'une représentation adéquate au sein des comités pertinents.

123*

La direction opérationnelle est responsable de l'application cohérente à l'échelle de l'entreprise du concept cadre aux principaux produits, activités, processus et systèmes existants ainsi qu'aux nouveaux, et de son actualisation.

b) Principe 2 : concept cadre et système de contrôle

124*

Le concept cadre doit être transposé de manière adéquate et complète dans les prescriptions internes adoptées par le conseil d'administration et comprendre des précisions spécifiques à l'entreprise tenant compte des définitions prudentielles de risque opérationnel et de perte opérationnelle[7].

125*

Le concept cadre doit au moins intégrer les aspects suivants :

a. structures de la gestion des risques opérationnels, y compris les compétences, les obligations de rendre compte et les lignes de reporting ;

b. définition des instruments d'identification, de mesure, d'évaluation, de pilotage et d'établissement des rapports et de leur utilisation ;

c. détermination de la propension et de la tolérance au risque en fonction des types pertinents de risques opérationnels ; fixation des valeurs-seuils et/ou des limites ; définition des stratégies et instruments d'atténuation des risques ;

d. approche de la banque destinée à identifier les risques inhérents (les risques avant prise en compte des contrôles) ainsi qu'à fixer et à surveiller les valeurs-seuils et/ou les limites pour les risques résiduels (les risques après prise en compte des contrôles) ;

e. instauration de systèmes de production de rapports de risque et d'information du management (MIS) pour les risques opérationnels ;

f. définition d'une classification uniforme des risques opérationnels matériels pour assurer la cohérence au niveau de l'identification des risques, de leur évaluation et de la fixation des objectifs au sein de la gestion opérationnelle des risques ;[8]

g. garantie d'une évaluation et d'une vérification indépendantes appropriées des risques

[7] On entend par pertes opérationnelles les pertes liées à l'inadéquation ou à la défaillance de procédures internes, aux personnes ou aux systèmes ou encore à des facteurs externes. Sont compris les risques juridiques, contrairement aux risques stratégiques et de réputation (art. 89 OFR).

[8] L'absence de classification uniforme des risques opérationnels est susceptible d'entraîner une hausse de la probabilité que les risques ne soient ni identifiés ni catégorisés ou qu'aucune responsabilité ne soit affectée à l'évaluation, à la surveillance, au contrôle et à l'atténuation des risques.

opérationnels ;

~~a.~~h. obligation de vérifier et d'adapter en temps réel le concept cadre en cas de modification essentielle de la situation de risque.

126*

Les banques doivent disposer d'un système de contrôle documenté adéquat qui se décompose en règles, processus et systèmes. Par ailleurs, elles doivent implémenter des contrôles internes ainsi que des stratégies appropriées de transfert et d'atténuation des risques.

c) Principe 3 : identification, limitation et surveillance

127*

L'identification, la limitation et la surveillance des risques constituent la base d'un système de gestion des risques efficace. Une identification des risques efficace prend en compte aussi bien des facteurs internes[9] qu'externes[10]. Des exemples d'instruments et de méthodes susceptibles d'être utilisés pour identifier et évaluer les risques opérationnels peuvent ainsi être :

a. les évaluations de risques et de contrôles ;

b. les résultats de la révision ;

c. la collecte et l'analyse des données internes relatives aux pertes ;

d. la collecte et l'analyse des événements externes avec des risques opérationnels ;

e. l'analyse des rapports entre risques, processus et contrôles ;

f. les indicateurs de risque et de performance pour la surveillance des risques opérationnels et pour l'efficacité du système de contrôle interne ;

g. les analyses de scénarios ;

h. la mesure et la quantification du potentiel de perte ;

~~a.~~i. les analyses comparatives[11].

128*

La banque doit veiller au fait que les mécanismes régissant la fixation des prix en interne (pricing) et la mesure de la performance tiennent compte de manière appropriée des risques opérationnels.

[9] Par exemple, structure de l'entreprise, nature des activités, qualifications des collaborateurs, changements sur le plan et fluctuation de l'effectif d'une banque.

[10] Par exemple, modifications de l'environnement élargi et de la branche ainsi qu'avancées technologiques.

[11] Lors d'une analyse comparative, les résultats des différents instruments d'évaluation sont croisés afin d'obtenir une vue plus complète des risques opérationnels de la banque.

d) Principe 4 : établissement de rapports internes et externes

129*

La direction opérationnelle doit implémenter un processus de surveillance permanente du profil des risques opérations et des principaux risques de perte. Au niveau du conseil d'administration, de la direction opérationnelle et des segments d'affaires, il faut instaurer des mécanismes de production de rapports propres à contribuer à une gestion proactive des risques opérationnels.

130*

L'établissement de rapports internes sur les risques opérationnels peut intégrer des données concernant la finance, l'exploitation et la compliance, mais aussi des informations externes pertinentes pour le risque et ayant trait à des événements et conditions qui ont un rôle essentiel pour la prise de décision. Le rapport sur les risques opérationnels doit au moins comprendre les points suivants et présenter leurs répercussions possibles sur la banque et le capital propre requis pour les risques opérationnels :

a. les entorses vis-à-vis de la propension au risque définie et de la tolérance aux risques ainsi que le dépassement des valeurs-seuils et/ou des limites définies à ce sujet pour les types pertinents de risques opérationnels ;

b. les détails sur les événements internes significatifs liés aux risques opérationnels et/ou les pertes ;

~~a.~~c. les informations relatives aux événements externes pertinents et aux risques potentiels ainsi qu'à leurs possibles répercussions sur la banque.

131*

Une banque doit disposer d'une politique de déclaration formelle, approuvée par le conseil d'administration. Cette dernière doit indiquer l'approche adoptée par la banque dans le cadre de la déclaration des risques opérationnels et les processus de contrôle qu'il faut appliquer en matière de déclaration. Par ailleurs, il convient d'implémenter un processus qui garantit l'adéquation du contenu et de la fréquence des déclarations et réglemente la vérification périodique de ces dernières.

132*

Les informations que les banques doivent déclarer en externe doivent permettre aux groupes d'interlocuteurs de se former un jugement sur l'approche relative à la gestion des risques opérationnels. Le concept pour la gestion des risques opérationnels en fait notamment partie. Il doit donner aux groupes d'interlocuteurs la possibilité d'évaluer l'efficacité de l'identification, de limitation et de surveillance des risques opérationnels.

e) Principe 5 : infrastructure technologique

133* Afin d'appuyer la gestion des risques opérationnels, la direction opérationnelle doit se doter d'une infrastructure technologique[12] adéquate, tenant compte des besoins commerciaux actuels et à plus long terme. A cet effet, elle met à disposition les capacités suffisantes pour répondre tant aux exigences de l'exploitation ordinaire qu'à celles des phases de crise. Elle doit en outre garantir la sécurité, l'intégrité et la disponibilité des données et systèmes et implémenter une gestion des risques globale et intégrée.

f) Principe 6 : continuité en cas d'interruption de l'activité

134* La direction opérationnelle doit disposer de plans de maintien des affaires de la banque qui garantissent la continuité des activités et la délimitation des dommages en cas d'interruption grave de l'activité.[13]

C. Exigences qualitatives spécifiques au risque

135* Les risques opérationnels spécifiques, notamment ceux touchant au modèle commercial (p. ex. les risques opérationnels liés au traitement des données des clients ou des activités transfrontières) exigent un pilotage ainsi qu'un contrôle des risques opérationnels plus étendus et plus intenses que ceux prescrits dans les exigences qualitatives de base. La direction opérationnelle est généralement tenue d'implémenter toute autre mesure requise pour garantir une surveillance adéquate de ces risques.

136* Si la FINMA le considère nécessaire, elle peut définir d'autres concrétisations en matière de gestion des risques opérationnels pour des thèmes spécifiques. Elles sont adoptées avec retenue et en application du principe de proportionnalité. D'autres exigences qualitatives classées par thème sont publiées dans l'annexe à la présente circulaire.

V. Audit et évaluation par les sociétés d'audit

137* Les sociétés d'audit vérifient le respect de la présente circulaire sur la base de la Circ.-FINMA 13/3 « Activités d'audit » et consignent le résultat de leurs opérations d'audit dans le rapport correspondant.

[12] Par infrastructure technologique, on entend la structure (électronique) physique et logique des systèmes IT et de communication les différentes composantes matérielles et logicielles, les données et l'environnement d'exploitation.

[13] Les chiffres 5.4.1 *Business Impact Analysis* et 5.4.2 *Business Continuity Strategy* des Recommandations de l'ASB en matière de *Business Continuity Management* (BCM) du 14 novembre 2007 sont reconnus comme standards minimaux conformément à la Circ.-FINMA 08/10 « Normes d'autorégulation reconnues comme standards minimaux ».

~~Annexe 1~~

~~Exigences qualitatives de base~~

~~Les exigences ci-après s'appliquent à l'ensemble des banques, au plus tard à partir du 1er janvier 2008, à l'exception de celles qui utilisent l'approche de l'indicateur de base et ne répondent à aucun des deux critères figurant aux Cm 21 et 22. Elles représentent la mise en œuvre concrète en Suisse du document « Sound Pratices for the Management and Supervision of operational Risk » publié en février 2003 par le Comité de Bâle sur le contrôle bancaire.~~ 1

1. ~~L'organe exerçant la haute direction, la surveillance et le contrôle doit être conscient des principaux risques opérationnels de sa banque. Il doit – directement ou par le biais d'un comité – avaliser les principes écrits régissant le comportement envers les risques opérationnels et les vérifier périodiquement. Ces principes ont pour objet l'identification, l'analyse, la surveillance et le contrôle des risques opérationnels, de même que les mesures visant à atténuer l'exposition aux risques opérationnels.~~ 2

2. ~~L'organe exerçant la haute direction, la surveillance et le contrôle veille à ce que la révision interne vérifie les principes régissant le comportement envers les risques opérationnels. Les fonctions relatives à la gestion des risques opérationnels ne peuvent pas être assumées directement par la révision interne.~~ 3

3. ~~La responsabilité de la mise en œuvre des principes régissant le comportement envers les risques opérationnels au sein de la banque incombe à la direction générale. Celle-ci doit veiller à la mise en œuvre cohérente des principes dans l'ensemble de la structure d'organisation et faire en sorte que tous les collaborateurs soient conscients de leur responsabilité en matière de comportement envers les risques opérationnels. En outre, il incombe à la direction générale d'élaborer des mesures pour la gestion des risques opérationnels découlant de l'ensemble des activités de la banque.~~ 4

4. ~~Les banques doivent pouvoir identifier et apprécier les risques opérationnels inhérents à l'ensemble de leurs activités, produits, processus et systèmes. Avant de procéder à une modification de la structure des activités, produits, processus et systèmes, elles doivent juger celle-ci de manière adéquate sous l'angle des risques opérationnels.~~ 5

5. ~~Les banques doivent surveiller systématiquement leur profil de risque opérationnel et leurs risques opérationnels matériels. La direction générale et l'organe assurant la haute direction, la surveillance et le contrôle sont informés des résultats obtenus afin de pouvoir, le cas échéant, prendre des mesures à titre proactif.~~ 6

6. ~~Les banques doivent disposer de concepts et de mesures concrètes pour la surveillance et/ou l'atténuation des risques opérationnels matériels. Ceux-ci doivent concorder avec la situation actuelle de la banque.~~ 7

7. ~~Les banques doivent mettre en place des plans de secours qui leur permettent de poursuivre leurs activités également dans des circonstances exceptionnelles et donc de limiter les conséquences de perturbations graves de leur activité normale.~~ 8

Annexe ~~21~~ 21*

finma

Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR

I. Vue d'ensemble

1

1er niveau	2e niveau	Activités
Financement et conseil d'entreprises	Financement et conseil d'entreprises	Fusions-acquisitions, émissions et placements, privatisations, titrisations, analyse, crédits (collectivités publiques, haut rendement), participations, prêts consortiaux, introductions en bourse (« Initial Public Offerings »), placements privés sur le marché secondaire
	Collectivités publiques	
	Banque d'affaires (« merchant banking »)	
	Prestations de conseil	
Négoce	Négoce pour compte de clients	Emprunts, actions, change, matières premières, crédits, dérivés, financement (« funding »), négoce pour compte propre, prêts et mises en pension de titres (repos), courtage (pour des investisseurs n'appartenant pas à la clientèle de détail), courtage de premier rang (« prime brokerage »)
	Tenue de marché	
	Négoce pour compte propre	
	Trésorerie	
Affaires de la clientèle privée	Banque de détail	Placements et crédits, prestations de services, opérations fiduciaires et conseil en placement
	Banque privée	Placements et crédits, prestations de services, opérations fiduciaires, conseil en placement et autres prestations de banque privée
	Prestations de service en matière de cartes	Cartes pour les entreprises et les particuliers
Affaires de la clientèle commerciale	Affaires de la clientèle commerciale	Financement de projets, financements immobiliers, financements d'exportations, financement du négoce, affacturage, leasing, octrois de crédits, garanties et cautionnements, effets de change
Trafic des paiements/règlement de titres[14]	Clientèle externe	Opérations de paiement, compensation et règlement d'opérations sur titres pour des tiers
Fonction d'agent	Garde de titres (« custody »)	Conservation à titre fiduciaire, dépôt, garde de titres, prêts/emprunts de titres pour des clients; prestations similaires pour les entreprises
	Prestation d'agent aux entreprises	Fonctions d'agent émetteur et payeur
	Service de fiducie aux entreprises (« corporate trust »)	

[14] Les pertes subies à ce titre par un établissement dans le cadre de ses propres activités sont intégrées dans les pertes du segment d'affaires concerné.

Annexe ~~21~~ 21*

finma

Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR

Gestion d'actifs institutionnelle	Gestion d'actifs discrétionnaire	Gestion centralisée, segmentée, relative à la clientèle de détail, institutionnelle, fermée, ouverte, « private equity »
	Gestion d'actifs non discrétionnaire	Gestion centralisée, segmentée, relative à la clientèle de détail, institutionnelle, fermée ouverte
Opérations de commissions sur titres	Exécution d'ordres sur titres	Exécution, y compris toutes les prestations de service liées

II. Principes de répartition

1. Chacune des activités d'une banque doit être intégralement attribuée à l'un des huit segments d'affaires (1er niveau dans le tableau 2). L'attribution ne doit pas provoquer de chevauchements. 2

2. Les activités à caractère auxiliaire qui n'ont pas de rapport direct avec les affaires d'une banque à proprement parler sont également attribuées à un segment d'affaires. Si l'assistance fournie concerne un seul segment d'affaires, l'activité sera également attribuée à ce dernier. Lorsque plusieurs segments d'affaires sont desservis par une activité auxiliaire, l'attribution aura lieu sur la base de critères objectifs. 3

3. Si une activité ne peut pas être classée dans un segment d'affaires particulier sur la base de critères objectifs, elle sera attribuée au segment d'affaires présentant le facteur β le plus élevé parmi ceux entrant en ligne de compte. Cela s'applique également aux activités présentant un caractère auxiliaire. 4

4. Les banques peuvent utiliser des méthodes d'imputation internes pour la ventilation de leur indicateur de revenus GI. Cependant, la somme des indicateurs de revenus des huit segments d'affaires doit correspondre dans tous les cas à l'indicateur de revenus de l'ensemble de la banque tel qu'il est utilisé dans l'approche de l'indicateur de base. 5

5. La répartition d'activités sur les différents segments d'affaires en vue du calcul des exigences de fonds propres au titre des risques opérationnels doit être en principe compatible avec les critères utilisés pour la délimitation des risques de crédit et de marché. Toute exception à ce principe doit être justifiée avec précision et documentée. 6

6. L'ensemble du processus de classification doit être documenté avec précision. Les définitions écrites des segments d'affaires doivent être en particulier suffisamment claires et détaillées pour que des personnes étrangères à la banque soient à même de les appréhender. Lorsque des dérogations aux principes de classification sont possibles, celles-ci doivent être justifiées et documentées avec précision. 7

7. La banque doit disposer de procédures lui permettant de classifier de nouvelles activités ou de nouveaux produits. 8

8. La responsabilité des principes de classification incombe à la direction générale. Ceux-ci sont soumis à l'approbation de l'organe exerçant la haute direction, la surveillance et le contrôle. 9

9. Les procédures de classification seront vérifiées régulièrement par la société d'audit. 10

Annexe ~~3~~2*

Vue d'ensemble pour la classification des types d'événements

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
Fraude interne	Pertes dues à des actes visant à frauder, à détourner des biens ou à contourner des lois, des prescriptions ou des dispositions internes (avec l'implication d'au moins une partie interne à l'entreprise)	Activité non autorisée	Transactions non notifiées (intentionnellement) Transactions non autorisées (avec préjudice financier) Saisie (intentionnellement) erronée de positions
		Vol et fraude	Fraude, fraude au crédit, dépôts sans valeur Vol, extorsion et chantage, abus de confiance, brigandage Détournement de biens Destruction malveillante de biens Contrefaçons Falsification de chèques Contrebande Accès non autorisé à des comptes de tiers Délits fiscaux Corruption Délits d'initié (pas pour le compte de l'entreprise)
Fraude externe	Pertes dues à des actes visant à frauder, à détourner des biens ou à contourner des lois ou des prescriptions (sans le concours d'une partie interne à l'entreprise)	Vol et fraude	Vol, brigandage Contrefaçons Falsification de chèques
		Sécurité des systèmes informatiques	Dommages dus au piratage informatique Accès non autorisé à des informations (avec préjudice financier)
Poste de travail	Pertes résultant d'actes contraires aux dispositions légales relatives au travail ou aux prescriptions ou conventions relatives à la sécurité ou à la santé, y compris l'ensemble des versements en rapports avec de tels actes	Collaborateurs	Versements compensatoires et d'indemnisation, pertes liées à des grèves, etc.
		Sécurité au poste de travail	Responsabilité civile Infractions aux dispositions relatives à la sécurité et à la santé du personnel Indemnisations ou dommages-intérêts versés au personnel

Annexe ~~3~~2*

Vue d'ensemble pour la classification des types d'événements

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
		Discrimination	Dommages-intérêts versés au titre d'actions en discrimination
Clients, produits et pratiques commerciales	Pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à des obligations envers des clients et pertes résultant de la nature et de la structure de certains produits	Conformité, diffusion d'informations et devoir fiduciaire	Violation du devoir fiduciaire, non-respect de directives Problèmes posés par la conformité et la diffusion d'informations (règles du « Know-your-Customer », etc.) Violation du devoir d'informer la clientèle Violation du secret professionnel du banquier ou de dispositions relatives à la protection des données Pratiques de vente agressives Création inappropriée de commissions et de courtage Utilisation abusive d'informations confidentielles Responsabilité du prêteur
		Pratiques commerciales ou de place incorrectes	Violation de dispositions antitrust Pratiques de place illicites Manipulation du marché Délits d'initié (pour le compte de l'entreprise) Activités commerciales sans autorisation correspondante Blanchiment d'argent
		Problèmes avec des produits	Problèmes liés à des produits (absence de pouvoirs, etc.) Fautes en matière de modèles

Annexe ~~3~~2*

Vue d'ensemble pour la classification des types d'événements

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
		Sélection des clients, attribution d'affaires et exposition de crédit	Procédés d'analyse de la clientèle incompatibles avec les directives internes Dépassement de limites
		Activités de conseil	Litiges en rapport avec les résultats d'activités de conseil
Dommage aux actifs corporels	Pertes résultant de dommages causés à des actifs physiques par des catastrophes naturelles ou d'autres événements	Catastrophes ou autres événements	Catastrophes naturelles Terrorisme Vandalisme
Interruptions d'activité et dysfonctionnement de systèmes	Pertes résultant de perturbations de l'activité ou de problèmes liés à des systèmes techniques	Systèmes techniques	Matériel informatique Logiciels Télécommunications Pannes d'électricité, etc.
Exécution, livraison et gestion des processus	Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus; pertes subies dans le cadre des relations avec les partenaires commerciaux, les fournisseurs, etc.	Saisie, exécution et suivi des transactions	Problèmes de communication Erreurs lors de la saisie ou dans le suivi des données Dépassement d'un délai Non-exécution d'une tâche Erreurs dans l'utilisation d'un modèle ou d'un système Erreurs comptables ou affectation à une fausse unité Livraison erronée ou non effectuée Gestion inappropriée d'instruments de couverture Erreurs dans la gestion des données de référence Erreurs concernant d'autres tâches
		Surveillance et annonces	Non-respect de devoirs d'annoncer Rapports inadéquats remis à des externes (ayant entraîné une perte)

Annexe ~~3~~2*

Vue d'ensemble pour la classification des types d'événements

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
		Admission de clientèle et documentation	Non-respect des règles internes et externes en la matière
		Gestion de comptes clients	Octroi illégitime de l'accès à un compte Tenue du compte incorrecte ayant entraîné une perte Négligences ayant entraîné la perte ou la détérioration d'actifs de clients
		Partenaires commerciaux	Prestation déficiente de partenaires commerciaux (hors clientèle) Litiges divers avec des partenaires commerciaux (hors clientèle)
		Fournisseurs	Sous-traitance (outsourcing) Litiges avec des fournisseurs

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

~~Cm de la Circ.~~	~~§ document Com. Bâle~~[15]	~~Teneur et commentaire éventuel quant à l'application en Suisse~~
~~1~~	~~645~~	~~Objet et but de la Circulaire~~
~~2~~	~~644~~	~~Définition de la notion de risque opérationnel~~
~~–~~	~~646~~	~~Encouragement à passer aux approches plus élaborées : ne figure pas dans la Circulaire.~~
~~–~~	~~647~~	~~Souhait que certaines banques n'appliquent pas l'approche de l'indicateur de base (BIA) : ne figure pas dans la Circulaire. Evocation de la possibilité d'une application partielle.~~
~~3~~	~~649~~	~~Explication des exigences de fonds propres pour la BIA : texte~~
~~4~~	~~–~~	~~Définition de la notion des trois années qui précèdent~~
~~5~~	~~649~~	~~Explication des exigences de fonds propres pour la BIA : formule~~
~~6~~	~~649~~	~~Explications de la formule figurant au Cm 5~~
~~7~~	~~649~~	~~Explications de la formule figurant au Cm 5~~
~~8~~	~~649~~	~~Explications de la formule figurant au Cm 5~~
~~9~~	~~650~~	~~Définition suisse du GI (limitation de la prise en compte du produit des participations aux participations non consolidées)~~
~~10~~	~~650~~	~~Composantes du GI : produit des intérêts~~
~~11~~	~~650~~	~~Composantes du GI : résultat des opérations de commissions et des prestations de services~~
~~12~~	~~650~~	~~Composantes du GI : résultat des opérations de négoce~~
~~13~~	~~650~~	~~Composantes du GI : résultat des participations non consolidées~~
~~14~~	~~650~~	~~Résultat des immeubles~~
~~15~~	~~–~~	~~Explications relatives à la consolidation de l'indicateur des revenus GI~~
~~16~~	~~–~~	~~Explications relatives à l'adaptation de l'indicateur des revenus GI après modification de la structure d'une banque suite au développement ou à la réduction d'activités (par ex. après reprise ou aliénation de segments d'affaires~~
~~17~~	~~–~~	~~Possibilité d'autoriser d'autres normes comptables que celles de la Circ. FINMA 08/2 « Comptabilité – banques »~~
~~18~~	~~650~~	~~Traitement de l'externalisation (y compris la possibilité de déduire les charges engendrées par cette dernière en cas de consolidation commune avec le prestataire de services d'externalisation)~~
~~20~~	~~651~~	~~Exigences qualitatives de base pour la BIA (fondées sur les « *Sound Pratices for the Management and Supervision of operational Risk* ») : selon la Circulaire, uniquement pour les banques d'une certaine taille et les banques présentes à l'étranger.~~
~~21~~		~~Critère de la taille selon le Cm 20~~
~~22~~		~~Critère de la présence à l'étranger selon le Cm 20~~
~~23~~	~~652 et 654~~	~~Ventilation des huit segments d'affaires et de leurs facteurs β~~
~~24~~	~~654~~	~~Explication des exigences de fonds propres pour l'AS : texte~~
~~–~~	~~653~~	~~Différentes explications à propos du concept de l'approche standard (AS) : ne figure pas dans la Circulaire.~~
~~–~~	~~Note 97~~	~~Approche standard alternative : non appliquée en Suisse.~~
~~25~~	~~654~~	~~Explication des exigences de fonds propres pour l'AS : formule~~
~~26~~	~~654~~	~~Explications de la formule figurant au Cm 25~~
~~27~~	~~654~~	~~Explications de la formule figurant au Cm 25~~
~~28~~	~~651~~	~~Respect des exigences qualitatives de base (fondées sur les « *Sound*~~

[15] ~~Voir note 1 dans le texte principal.~~

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

~~Cm de la Circ.~~	~~§ document Com. Bâle~~[15]	~~Teneur et commentaire éventuel quant à l'application en Suisse~~
		~~*Pratices for the Management and Supervision of operational Risk »)*~~
~~29~~	~~662~~	~~Répartition des activités dans l'AS~~
~~30~~	~~663~~	~~Introduction sur les exigences posées aux banques présentes à l'étranger dans l'AS~~
~~31~~	~~663a~~	~~Système de gestion dans le domaine des risques opérationnels~~
~~32~~	~~663a~~	~~Système de gestion dans le domaine des risques opérationnels~~
~~33~~	~~663a~~	~~Système de gestion dans le domaine des risques opérationnels~~
~~34~~	~~663a~~	~~Système de gestion dans le domaine des risques opérationnels~~
~~35~~	~~663a~~	~~Système de gestion dans le domaine des risques opérationnels~~
~~36~~	~~663b~~	~~Système d'évaluation des risques opérationnels~~
~~37~~	~~663b~~	~~Système d'évaluation des risques opérationnels~~
~~38~~	~~663b~~	~~Système d'évaluation des risques opérationnels~~
~~39~~	~~663b~~	~~Système d'évaluation des risques opérationnels~~
~~40~~	~~663c~~	~~Notification aux organes dirigeants~~
~~41~~	~~663d~~	~~Documentation~~
~~42~~	~~663d~~	~~Documentation~~
~~43~~	~~663e~~	~~Validation et vérification~~
~~44~~	~~663f~~	~~Audit externe~~
~~45~~	~~655~~	~~Principe de base des approches spécifiques aux établissements (AMA)~~
~~46~~	~~655~~	~~Obligation d'obtenir une autorisation pour les AMA; mise en œuvre au plus tôt début 2008~~
~~47~~	~~659~~	~~Utilisation préalable de l'AMA à des fins de comparaison et de test (application parallèle et études d'impact)~~
~~48~~	~~648~~	~~Restrictions concernant le passage de l'AMA à la BIA ou à l'AS~~
~~49~~	~~–~~	~~Imputation des charges liées aux contrôles pour l'AMA~~
~~–~~	~~656~~	~~Prise en compte des mécanismes d'allocation : pas d'application explicite en Suisse.~~
~~–~~	~~657~~	~~Prise en compte des effets de diversification pour les banques étrangères autorisées à utiliser AMA dans le pays d'origine : pas de prise en compte explicite en Suisse.~~
~~–~~	~~658~~	~~Surveillance de l'adéquation du mécanisme d'allocation utilisé : superflu en Suisse.~~
~~OFR~~	~~659~~	~~Remarque à propos de l'utilisation de l'AMA dans le contexte global de Bâle III avec les planchers correspondants~~
~~–~~	~~660~~	~~Trois exigences à remplir pour l'AS : ne sont pas évoquées explicitement dans la Circulaire. Elles sont toutefois prises en compte, en particulier par le biais des exigences figurant dans les *« Sound Pratices for the Management and Supervision of operational Risk »* du février 2003~~
~~–~~	~~661~~	~~Période d'essai pour l'AS : il y est renoncé pour la mise en œuvre en Suisse.~~
~~50~~	~~651~~	~~Respect des exigences qualitatives de base (fondées sur les *« Sound Pratices for the Management and Supervision of operational Risk »*, février 2003)~~
~~51~~	~~664~~	~~Introduction relative aux exigences qualitatives pour AMA~~
~~52~~	~~664, point 1~~	~~Implication active de l'organe chargé de la haute direction, de la surveillance et du contrôle dans la surveillance~~
~~53~~		~~Familiarisation de la direction générale avec le concept de base~~
~~54~~	~~664, point 2~~	~~Système solidement conçu et mis en œuvre avec intégrité~~

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

~~Cm de la Circ.~~	~~§ document Com. Bâle~~[15]	~~Teneur et commentaire éventuel quant à l'application en Suisse~~
~~55~~	~~664, point 3~~	~~Ressources suffisantes~~
~~–~~	~~665~~	~~Différentes informations introductives~~
~~56~~	~~666a~~	~~Unité centrale indépendante pour la gestion des risques opérationnels~~
~~57~~	~~666a~~	~~Point se rapportant au Cm 56~~
~~58~~	~~666a~~	~~Point se rapportant au Cm 56~~
~~59~~	~~666a~~	~~Point se rapportant au Cm 56~~
~~60~~	~~666a~~	~~Point se rapportant au Cm 56~~
~~61~~	~~666b~~	~~Intégration dans le processus de gestion des risques~~
~~62~~	~~666b~~	~~Intégration dans le processus de gestion des risques~~
~~63~~	~~666b~~	~~Intégration dans le processus de gestion des risques~~
~~64~~	~~666c et d~~	~~Renvoi aux Cm 40–42~~
~~65~~	~~666e~~	~~Révision interne et externe~~
~~66~~	~~666f~~	~~Validation par l'autorité de surveillance et la société d'audit : en Suisse, uniquement par la société d'audit~~
~~67~~	~~666f~~	~~Point se rapportant au Cm 66~~
~~68~~	~~666f~~	~~Point se rapportant au Cm 66~~
~~69~~	~~667~~	~~Introduction à propos des exigences quantitatives : idée du concept de base libéral~~
~~70~~	~~667~~	~~Remarque à propos du quantile 99,9 %~~
~~–~~	~~668~~	~~Remarque à propos de la flexibilité et des normes rigoureuses ainsi que d'un éventuel remaniement ultérieur par le Comité de Bâle~~
~~71~~	~~669a~~	~~Compatibilité des définitions~~
~~72~~	~~669b~~	~~Evocation de la possibilité de déduire les pertes attendues~~
~~–~~	~~669c~~	~~Exigence de «granularité suffisante» : pas de mention explicite dans la Circulaire. La notion est problématique, et le respect de l'idée est assuré par les autres exigences.~~
~~73~~	~~669d~~	~~Prise en compte d'hypothèses de corrélation : mise en œuvre pragmatique dans la Circulaire. Prise au sens strict, la formulation du Comité de Bâle n'est pas applicable.~~
~~74~~	~~669e~~	~~Prise en compte des quatre facteurs d' « input »~~
~~75~~	~~669f~~	~~Concept pour l'intégration des quatre facteurs d' « input »~~
~~–~~	~~670~~	~~Introduction à propos des exigences régissant la collecte des données internes relatives aux pertes~~
~~76~~	~~671~~	~~Suivi de la collection de données relatives aux pertes~~
~~77~~	~~672~~	~~Durée minimale des périodes d'observation retenues~~
~~78~~	~~673~~	~~Introductions à propos des exigences posées à la procédure de création d'une base de données interne à l'établissement~~
~~79~~	~~673, point 1~~	~~Classification par segments d'affaires et types d'événements~~
~~80~~	~~673, point 2~~	~~Elaboration d'une base de données exhaustive; seuil~~
~~81~~	~~673, point 3~~	~~Informations à propos des données relatives aux pertes : selon la Circulaire, les causes de la perte ne doivent être expliquées qu'à partir d'un montant brut de 1 million de CHF.~~
~~82~~	~~673, point 4~~	~~Principes pour le recensement des événements générateurs de pertes~~
~~83~~	~~673, point 5~~	~~Pertes opérationnelles associées au risque de crédit~~
~~84~~	~~673, point 6~~	~~Pertes opérationnelles associées au risque de marché; mention explicite de l'obligation de prendre en compte de telles pertes dans un éventuel modèle de risque de marché~~
~~85~~	~~–~~	~~Gestion des pertes opérationnelles « négatives » : pas de mention explicite dans le texte du Comité de Bâle.~~

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

~~Cm de la Circ.~~	~~§ document Com. Bâle~~[15]	~~Teneur et commentaire éventuel quant à l'application en Suisse~~
~~86~~	~~674~~	~~But des données de pertes externes~~
~~87~~	~~674~~	~~Informations relatives aux différentes données de pertes externes~~
~~88~~	~~674~~	~~Méthodologie pour l'utilisation des données de pertes externes~~
~~89~~	~~675~~	~~Obligation de prendre en compte l'analyse de scénarios~~
~~90~~	~~675~~	~~Idée de base de l'analyse de scénarios~~
~~91~~	~~675~~	~~Vérification et mise à jour régulières des scénarios : selon la Circulaire, au moins une fois par an ou directement après un changement significatif de la situation en matière de risque.~~
~~92~~	~~676~~	~~Idée de base des facteurs relatifs à l'environnement opérationnel et au système de contrôle interne.~~
~~93~~	~~676~~	~~Introduction au sujet des exigences~~
~~94~~	~~676, point 1~~	~~Choix des facteurs relatifs à l'environnement opérationnel et au système de contrôle interne~~
~~95~~	~~676, point 2~~	~~La sensibilité des estimations relatives au risque de modifications de facteurs de l'environnement opérationnel et du système de contrôle interne doit être justifiable et vérifiable~~
~~96~~	~~676, point 3~~	~~Documentation~~
~~97~~	~~676, point 4~~	~~Validation~~
~~98~~	~~677~~	~~Prise en compte en principe de l'effet de couverture des contrats d'assurance; limitation à 20 %~~
~~99~~	~~678~~	~~Introduction au sujet des conditions~~
~~100~~	~~678, point 1~~	~~Notation minimale du donneur d'assurance~~
~~101~~	~~678, point 2; 679, point 1~~	~~Durée initiale minimale, durée résiduelle minimale et précision des «réductions (« haircuts ») appropriées» : de façon linéaire dans la Circulaire.~~
~~102~~	~~678, point 3; 679, point 2~~	~~Délai de résiliation minimal de 90 jours et gestion des décotes lorsque le délai de résiliation est inférieur à un an : de façon linéaire dans la Circulaire.~~
~~103~~	~~678, point 4~~	~~Clauses restrictives et d'exclusion en cas d'intervention de l'autorité de régulation~~
~~104~~	~~678, point 5~~	~~Transparence du calcul de l'effet de couverture~~
~~105~~	~~678, point 6~~	~~Assurance par des prestataires non externes~~
~~106~~	~~678, point 7~~	~~Orientation d'après le transfert de risque effectif et documentation~~
~~107~~	~~678, point 8~~	~~Obligation de publier des informations sur le recours à des solutions d'assurance~~
~~–~~	~~679, point 3~~	~~Incertitude concernant l'indemnisation et absence éventuelle de la couverture fournie : pas de mention explicite dans la Circulaire. Respect du principe déjà assuré par les autres exigences.~~
~~108~~	~~680~~	~~En principe, possibilité d'appliquer partiellement AMA~~
~~109~~	~~680, point 1/2~~	~~Couverture intégrale~~
~~110~~	~~680, point 3~~	~~Couverture au moment de la mise en oeuvre~~
~~111~~	~~680, point 4~~	~~Calendrier pour l'extension de l'application de l'AMA~~
~~112~~	~~680, point 4~~	~~La BIA et l'AS ne peuvent pas être conservées dans certains secteurs pour des raisons d'optimisation des fonds propres. La Circulaire formule explicitement l'idée exprimée dans la dernière phrase du §680, point 4.~~
~~113~~	~~681~~	~~Délimitation entre les différentes approches~~
~~114~~	~~–~~	~~Mention explicite de l'interdiction d'appliquer différentes approches~~

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

~~Cm de la Circ.~~	~~§ document Com. Bâle~~[15]	~~Teneur et commentaire éventuel quant à l'application en Suisse~~
		~~pour calculer les exigences de fonds propres découlant des risques opérationnels~~
~~–~~	~~682~~	~~AMA : règlementation spéciale pour les filiales étrangères de banques n'appliquant pas l'AMA de manière consolidée au niveau du groupe : n'est pas prise en compte dans la Circulaire.~~
~~–~~	~~683~~	~~Remarque concernant le caractère restrictif des cas approuvés selon le §682 : insignifiant pour la mise en œuvre en Suisse.~~
~~115~~	~~778; notes 98 et 99~~	~~Interventions au titre du 2e pilier~~
~~116~~	~~–~~	~~Date d'entrée en vigueur~~
~~Annexe 1~~	~~Document séparé~~	~~Exigences qualitatives de base : représente la mise en œuvre en Suisse des « *Sound Pratices for the Management and Supervision of operational Risk* » du Comité de Bâle du février 2003~~
~~Annexe 2A~~	~~Annexe 6~~	~~Classification des segments d'affaires : vue d'ensemble~~
~~Annexe 2B~~	~~Annexe 6~~	~~Classification des segments d'affaires : répartition~~
~~–~~	~~Note 2, Annexe 6~~	~~Indications additionnelles pour la ventilation (« mapping ») entre les segments d'affaires : pas de mention explicite dans la Circulaire.~~
~~Annexe 3~~	~~Annexe 7~~	~~Vue d'ensemble pour la classification des types d'événements~~

1*

La présente annexe énonce les principes de 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 (« données des clients »), ainsi que les précisions y afférentes. Ces principes se concentrent principalement sur le risque d'incidents en relation avec la confidentialité des données de clients en masse 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 d'intégrité et de disponibilité des données. Les dispositions juridiques pertinentes ne trouvent pas seulement leur source dans le droit de la surveillance[16], mais aussi dans la législation relative à la protection des données[17] et dans le droit civil.

2*

Les petites[18] 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.

[16] Notamment art. 3 et 47 LB ainsi qu'art. 9 OB ; art. 10 et 43 LBVM ainsi qu'art. 19 s. OBVM.
[17] 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).
[18] Cf. Cm 118 du chapitre IV. A.

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

I. Principes de bonne gestion des risques en lien avec la confidentialité des données des clients.

A. Principe 1 : gouvernance

3*

Les risques en lien avec la confidentialité des données de clients sont systématiquement identifiés, limités et surveillés. A cet effet, le conseil d'administration surveille la direction opérationnelle pour s'assurer d'une implémentation efficace des mesures destinées à garantir la confidentialité des données des clients. La direction opérationnelle mandate un organe de contrôle indépendant pour établir et préserver les conditions-cadre garantissant la confidentialité des données des clients.

a) Indépendance et responsabilité

4*

L'unité compétente pour l'établissement et la préservation des conditions-cadre garantissant la confidentialité des données des clients doit être indépendante des unités qui sont responsables du traitement des données. Elle peut faire partie de l'organisation de contrôle des risques ou de toute unité équivalente pour autant qu'elle soit indépendante des unités qui sont responsables du traitement des données des clients. Selon la taille et la complexité de la banque, l'unité compétente peut également être assistée de plusieurs unités décentralisées.

5*

Les responsabilités doivent être définies pour l'ensemble des fonctions et des sites impliqués et des structures claires de remontée des informations doivent être mises en place. La définition des responsabilités et leur répartition entre les fonctions *Front Office*, IT ou de contrôle doivent notamment être établies par la direction opérationnelle, puis approuvées par le conseil d'administration. La direction opérationnelle informe régulièrement le conseil d'administration de l'efficacité des contrôles introduits.

b) Règles, processus et systèmes

6*

Il faut qu'il existe un concept cadre formel et complet des activités, processus et systèmes garantissant la confidentialité des données dont la structure tient compte de la taille et de la complexité de la banque. Ce concept cadre doit être mis en œuvre de manière cohérente dans l'ensemble des domaines fonctionnels et des unités qui ont accès ou traitent aux données des clients.

7*

L'implémentation et le respect du concept cadre relatif à la confidentialité des données des clients doivent être soumis à la surveillance du conseil d'administration et être garantis par des contrôles réguliers de l'unité compétente pour la confidentialité et la sécurité des données.

B. Principe 2 : données d'identification du client (*client identifying data*, CID)

8*

L'exigence fondamentale à laquelle doit répondre un concept cadre adéquat garantissant la confidentialité des données des clients tient dans la catégorisation des données de clients traitées par une banque. Elle requiert de l'entreprise la définition spécifique de données

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

d'identification des clients (CID) et leur classification en fonction de leur niveau de confidentialité et de protection. Il faut également régler l'attribution de la responsabilité des données (« Data Owners »).

a) Catégories de données de clients et définition des CID

9*

Une liste claire et transparente des catégories de données de clients, incluant la définition des CID spécifique à l'entreprise, doit exister au sein de la banque et être documentée sur le plan formel. La catégorisation et la définition des données des clients doit englober la totalité des données d'identification directe des clients (p. ex. prénom, deuxième nom, nom de famille), des données d'identification indirectes des clients (p. ex. numéro de passeport) et des données d'identification potentiellement indirecte des clients (p. ex. combinaison de la date de naissance, de la profession, de la nationalité, etc.).

10*

Toute banque doit disposer d'une catégorisation et d'une définition des CID qui lui sont propres et appropriées à sa base de clientèle spécifique. Le chapitre III comprend une liste non exhaustive d'exemples.

b) Classification des CID et niveaux de confidentialité

11*

Les CID doivent être réparties en niveaux de confidentialité en fonction de critères de classification formels. A des fins de protection des données, la classification des données des clients doit intégrer des exigences claires concernant l'accès et les mesures techniques correspondantes (p. ex. anonymisation, chiffrement ou pseudonymisation) et distinguer en principe différents niveaux de confidentialité et de protection.

12*

En se basant sur les exemples présentés au chapitre III, on part du principe qu'au moins les CID directes (catégorie A) et une sélection de CID indirectes (p. ex. numéro de passeport dans la catégorie B) appartiennent à un niveau supérieur[19] de sécurité et de confidentialité des données des clients. Dans le cas d'une banque qui ne connaît qu'une seule catégorie, il convient d'appliquer un niveau supérieur de protection et de confidentialité des données des clients à la totalité des CID.

c) Responsabilité des CID

13*

Des critères uniformément applicables à toutes les unités qui ont accès à des CID ou qui traitent ces dernières doivent être définis pour l'attribution de la responsabilité des données. Les unités responsables des CID (« Data Owners ») doivent assumer la surveillance de la totalité du cycle de vie des données des clients, incluant la validation des droits d'accès ainsi que la suppression et le retraitement des systèmes opérationnels et de sauvegarde.

14*

Les unités responsables des CID (« Data Owners ») sont chargées de l'implémentation des

[19] Le niveau supérieur de protection et de confidentialité des données des clients ne doit pas impérativement être le niveau le plus élevé de protection et de confidentialité qu'un établissement connaît pour l'information. Il doit toutefois tenir compte du fait qu'une violation de la confidentialité des données des clients peut entraîner une détérioration grave de la situation économique ou de la position sociétale des parties concernées.

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

directives de classification des données ainsi que de la justification et de la documentation des exceptions.

C. Principe 3 : lieu de stockage et accès aux données

15*

La banque doit connaître le lieu où les CID sont stockées, les applications et systèmes IT avec lesquels elles sont traitées et le lieu où il est possible d'y accéder par voie électronique. Il faut s'assurer par des contrôles appropriés que les données sont traitées conformément à l'art. 8 ss de l'ordonnance relative à la loi fédérale sur la protection des données. Des contrôles spéciaux sont nécessaires pour les domaines physiques (p. ex. salles de serveurs) ou les zones de réseaux au sein desquels de grandes quantités de CID sont stockées ou rendues accessibles. L'accès aux données doit être clairement réglementé et ne doit intervenir que sur une stricte base « need to know ».

a) Lieu de stockage et accès aux données en général

16*

Un inventaire des applications et de l'infrastructure y afférente (p. ex. base de données, sauvegardes) qui renferment ou traitent des CID doit être disponible et actualisé au fur et à mesure. L'inventaire doit aussi prendre en compte les applications et les CID qui sont utilisées à des fins de test (d'une nouvelle plate-forme IT p. ex.).

17*

On attend que la granularité de l'inventaire permette à la banque d'établir :

18*

- le lieu où les CID sont stockées, les applications et systèmes IT avec lesquels elles sont traitées et le lieu où il est possible d'y accéder par voie électronique (applications des utilisateurs finaux) ;

19*

- les sites et les unités juridiques au niveau national et international à partir desquels il est possible d'accéder aux données (y compris les prestations de service externalisées et les sociétés externes.

b) Lieu de stockage et accès aux données depuis l'étranger

20*

Lorsque les CID sont stockées hors de Suisse ou qu'elles font l'objet d'un accès depuis l'étranger (p. ex. en raison de transfert d'activités spécifiques au sein du groupe d'entreprises ou à des tiers externes), les risques accrus qui en résultent sur le plan de la protection des données des clients doivent être limités de manière appropriée.[20] Les CID doivent être protégées de manière adéquate (anonymisation, chiffrement ou pseudonymisation). Il convient d'adopter les mesures suivantes :

21*

- l'adoption de dispositifs de protection, leur implémentation et leur application doivent intervenir de manière adéquate ;

22*

- l'application de dispositifs de protection doit être surveillée par la définition de contrôles

[20] Il faut en outre respecter les dispositions déterminantes du droit de la protection des données, en particulier l'art. 6 LPD.

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

clés qui sont vérifiés périodiquement ;

23*

- les clients doivent être informés en détail, par courrier spécial, du transfert au sein du groupe ou à des tiers externes d'activités spécifiques qui sont réalisées à l'étranger et des dispositifs adoptés à des fins de protection de la confidentialité. Cette obligation est caduque lorsque les données disponibles hors de Suisse ne permettent pas de remonter à l'identité des clients concernés. Dans ce cas, les exigences générales relatives à l'information sur les activités externalisées au sens des principes 5 et 6 de la Circ.-FINMA 08/7 « Outsourcing – banques » sont suffisantes.

c) Principe du « need to know »

24*

Les personnes ne doivent avoir accès qu'aux informations et aux fonctionnalités nécessaires à l'exercice de leurs tâches. Il ne doit y avoir accès aux CID que si les unités responsables des CID (« Data Owners ») ont validé les droits d'accès. Les droits d'accès doivent être attribués comme suit :

25*

- Champ d'application : l'accès au CID doit être limité aux groupes de clients, segments, centres de comptabilisation ou autres sous-groupes de clients définis de manière appropriée auxquels le collaborateur concerné doit impérativement avoir accès dans le cadre de l'exercice de ses tâches.

26*

- Fonctions : l'autorisation d'accès est octroyée d'après la fonction (nature des tâches) que le collaborateur exerce en liaison avec les CID. Lorsque l'exercice d'une tâche ne requiert pas le traitement de CID (p. ex. établissement de rapports, analyse de données, conseil), il convient de restreindre l'autorisation d'accès (p. ex. par l'octroi de droits *read-only*).

27*

L'attribution des droits d'accès doit être régulièrement vérifiée.

d) Registre des accès

28*

La banque doit tenir un registre des collaborateurs et des tiers qui ont des autorisations d'accès aux CID. Le registre doit également mentionner les utilisateurs IT et usagers privilégiés (voir Cm 41 de la présente annexe). Seules les personnes inscrites dans ce registre sont autorisées à avoir accès aux CID.

29*

Des dispositifs tels que la tenue de fichiers-journaux doivent être introduits afin de permettre l'identification des utilisateurs qui ont eu accès à une grande quantité de CID.

D. Principe 4 : normes de sécurité liées à l'infrastructure et à la technologie

30*

Les normes de sécurité pour l'infrastructure et la technologie utilisées pour la protection de la confidentialité des CID doivent être en adéquation avec la complexité de la banque et l'exposition aux risques de cette dernière et garantir la protection des CID au niveau de l'appareil terminal (au point terminal) ainsi que des CID transférées et stockées. Les technologies de l'information étant soumises à des modifications rapides, il faut suivre avec attention l'évolu-

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

tion des solutions de sécurité des données. Il convient d'évaluer régulièrement les écarts entre le concept cadre existant en interne pour garantir la confidentialité des données des clients et la pratique du marché.

a) Normes de sécurité

31*

Les normes de sécurité doivent être en adéquation avec la taille de la banque et le degré de complexité de son architecture IT. En cas de normes de sécurité différenciées (p. ex. lorsque les normes de sécurité ne sont pas identiques pour tous les collaborateurs, processus ou instruments), il convient de définir et de documenter convenablement le rapport entre les normes supérieures de sécurité et la classification des données des clients.

b) Normes de sécurité et pratique du marché

32*

Les normes de sécurité sont une partie intégrante inamovible du concept cadre garantissant la confidentialité des données des clients. Ils doivent être confrontés régulièrement à la pratique du marché afin de repérer de potentielles lacunes de sécurité. Les contrôles indépendants et des rapports d'audit offrent également des inputs qu'il convient de prendre en compte.

c) Sécurité lors de la transmission des CID et au niveau des CID enregistrées sur l'appareil terminal (point terminal)

33*

Afin de garantir la confidentialité des CID, la banque doit examiner des mesures de protection (p. ex. chiffrement) et les mettre en œuvre, si nécessaires, aux niveaux suivants :

34*

a. sécurité des CID sur l'appareil terminal ou au point terminal (p. ex. ordinateurs, ordinateurs portables, supports de données portables et appareils mobiles) ;

35*

b. sécurité lors de la transmission des CID (p. ex. au sein d'un réseau ou entre les différents sites) ;

36*

c. sécurité des CID enregistrées (p. ex. sur les serveurs, dans les bases de données ou sur les supports de sauvegarde).

E. Principe 5 : sélection, surveillance et formation des collaborateurs qui ont accès aux CID

37*

Des collaborateurs bien formés et conscients de leur responsabilité représentent un élément central de la mise en œuvre à l'échelle de l'entreprise de mesures efficaces garantissant la protection de la confidentialité des données des clients. Il s'agit par conséquent de sélectionner avec soin les collaborateurs qui peuvent avoir accès aux CID, de les former et de les assujettir à une surveillance. Cela vaut également pour les tiers qui peuvent accéder aux CID, sur mandat de la banque. Des exigences supérieures de sécurité doivent s'appliquer aux utilisateurs IT et usagers privilégiés disposant d'un accès fonctionnel aux CID en masse (« collaborateurs clés »), auxquels il convient de prêter une attention particulière.

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

a) Sélection soigneuse des collaborateurs

38*

Les collaborateurs qui peuvent accéder aux CID doivent être sélectionnés avec soin. Il convient notamment de vérifier au moment de la prise d'activité que le collaborateur potentiel remplit les exigences qu'implique le traitement approprié des CID. Par ailleurs, la banque doit s'assurer que la sélection des collaborateurs par des tiers, de même que la désignation des collaborateurs par les entreprises tierces qui, sur mandat de la banque, peuvent accéder aux CID, répondent à un processus de sélection tout aussi soigneuse.

b) Formations ciblées des collaborateurs

39*

Les collaborateurs internes et externes doivent être sensibilisés aux questions relatives à la sécurité des données des clients dans le cadre de formations ciblées. En l'occurrence, il est attendu des collaborateurs qu'ils suivent un programme de sensibilisation quant à la confidentialité des données des clients. Ils doivent connaître le cadre établi pour la sécurité des données des clients et doivent notamment être informés du fait que la transmission de données de clients est punie par l'art. 47 LB.

c) Exigences de sécurité

40*

La banque doit disposer d'exigences claires en matière de sécurité pour les collaborateurs qui ont droit aux CID. Elle doit vérifier périodiquement si les exigences relatives à un traitement adéquat des CID sont toujours remplies. Des exigences supérieures de sécurité doivent s'appliquer aux utilisateurs IT et usagers privilégiés disposant d'un accès fonctionnel à une grande quantité de CID (« collaborateurs clés »), auxquels il convient de prêter une attention particulière.

d) Liste des collaborateurs clés

41*

En complément des exigences générales applicables aux collaborateurs ayant accès aux CID (voir Cm 28), la banque est tenue de tenir et d'actualiser au fur et à mesure une liste des noms de tous les utilisateurs IT et usagers privilégiés, internes et externes, qui ont un accès aux CID en masse et/ou auxquels des responsabilités en matière de contrôle et de surveillance de la confidentialité des données des clients ont été transférées. L'identité des utilisateurs IT et usagers privilégiés doit être connue du management suprême responsable au niveau local ou général.

e) Directive

42*

Les processus de sélection, de surveillance et de formation des collaborateurs qui ont accès à des CID doivent être définis dans une directive.

F. Principe 6 : identification et contrôle des risques en relation avec la confidentialité des CID

43*

L'unité compétente pour la confidentialité et la sécurité des données identifie et évalue les risques inhérents et les risques résiduels concernant la confidentialité des CID au moyen d'un

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

processus structuré. Ce processus doit comprendre les scénarios de risque[21] en relation avec la confidentialité des CID qui sont pertinents pour la banque et la définition des contrôles clés correspondants. Le catalogue des contrôles clés en relation avec la confidentialité des données afin de garantir la protection des CID doit être actualisé en permanence par des contrôles inédits ou améliorés.

a) Processus d'évaluation du risque

44*

L'évaluation du risque inhérent à la confidentialité des CID (risque sous-jacent, en l'absence de toute mesure de gestion ou de limitation) et du risque résiduel (qui prend en compte les mesures d'atténuation et de contrôle) doit intervenir sur la base d'un processus structuré et en impliquant les utilisateurs finaux ainsi que les fonctions informatiques et de contrôle. Elle peut avoir lieu dans le cadre d'un processus plus large d'auto-évaluation des risques et des contrôles qui intègre en plus les risques opérationnels.

b) Scénarios de risque et contrôles clés[22]

45*

La définition des scénarios de risque en lien avec la confidentialité des CID ainsi que les contrôles clés correspondants doivent être en adéquation avec l'exposition au risque et la complexité de la banque et être révisés périodiquement.

G. Principe 7 : limitation des risques en relation avec la confidentialité des CID

46*

Les risques identifiés doivent être surveillés et limités de manière appropriée. Ce principe vaut en particulier pour les activités au cours desquelles de grandes quantités de CID doivent être modifiées ou migrées.[23] Des mesures de sécurité appropriées et de niveau supérieur doivent être prévues dans ces cas de figure afin d'atténuer le risque d'incidents en relation avec la confidentialité des CID. Lors de changements structurels (p. ex. de réorganisations de grande ampleur), la banque doit se pencher sérieusement et suffisamment tôt sur les mesures de sécurité garantes de la confidentialité des CID.

a) Environnement de production, opérations portant sur une grande quantité de CID

47*

Les opérations qui, dans l'environnement productif, sont réalisées avec une grande quantité de CID qui ne sont pas anonymisées, chiffrées, ni pseudonymisées, doivent être soumises à des procédures appropriées (p. ex. principe du double contrôle et fichiers journaux), intégrant l'information de l'unité compétente pour la sécurité et la confidentialité des données. Il est at-

[21] Sur la base d'une analyse des incidents graves en relation avec la sécurité des données qui sont survenus au sein de la banque en elle-même ou chez des concurrents, ou d'une description d'incidents graves purement hypothétiques.

[22] 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).

[23] Ce cas de figure se présente notamment lors du développement, de la modification ou de la migration des systèmes du fait des avancées technologiques ou de restructurations organisationnelles.

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

tendu que, dans ces activités, soit inclus le travail des administrateurs IT, des collaborateurs ayant des droits d'accès supérieurs et des collaborateurs de tiers. Des requêtes de grande ampleur portant sur des CID – qui ne sont pas anonymisées, pseudonymisées ni chiffrées – et qui n'ont pas été approuvées ou des requêtes qui pourraient laisser penser à un comportement suspect doivent immédiatement être signalées au management suprême.

b) Tests pour le développement, les transformations et la migration des systèmes

48*

Pendant le développement, la transformation et la migration de systèmes, les CID doivent être protégées de manière adéquate contre l'accès et l'utilisation par des personnes non autorisées. Les techniques d'anonymisation, de pseudonymisation et de chiffrement (qu'elles soient développées en interne ou en externe) doivent faire l'objet de tests complets et d'une vérification périodique et être soumises à des contrôles stricts selon le principe du double contrôle. Avant leur application à des jeux de données importants, les tests doivent être limités à une série de jeux restreints de CID.

H. Principe 8 : incidents en rapport avec la confidentialité des CID, communication interne et externe

49*

Il est attendu des banques qu'elles introduisent des processus prédéfinis pour réagir rapidement à des incidents en relation avec la confidentialité, incluant une stratégie claire de communication des incidents graves. En outre, les exceptions, les incidents et les résultats des audits doivent être surveillés, analysés et signalés sous une forme appropriée au management suprême. Cette manière de procéder doit contribuer à l'amélioration permanente des mesures destinées à garantir la confidentialité des CID.

a) Identification des incidents en lien avec la confidentialité et réaction

50*

Il faut formaliser un processus clairement défini d'identification des incidents en rapport avec la confidentialité ainsi que la réaction qu'elle implique et les communiquer à toutes les parties concernées. Par ailleurs, l'ensemble des unités et sites qui ont accès à des CID doit disposer des ressources leur permettant de réagir aux incidents correspondants.

b) Annonce

51*

Il faut que le risque lié à la confidentialité des CID et les signalements de compliance s'y rapportant soient présentés de manière adéquate dans les rapports internes.

c) Amélioration permanente du cadre garantissant la confidentialité des CID

52*

Le concept cadre destiné à garantir la confidentialité des CID (Cm 6 et 7) et les standards de sécurité (Cm 31) doit être révisé périodiquement. Les incidents, exceptions et résultats des audits doivent contribuer à l'amélioration permanente de ce concept cadre.

d) Communication externe

53*

La banque doit disposer d'une stratégie de communication claire en cas d'incidents graves en

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

lien avec la confidentialité des CID. Il convient notamment de définir la forme et le moment précis de la communication à la FINMA, aux autorités de poursuite pénale, aux clients concernés et aux médias.

I. Principe 9 : externalisation d'activités et prestations de services à grande échelle traitant des CID

54*

La confidentialité des CID doit être un critère déterminant lors de la sélection des fournisseurs de prestations de service externalisées qui traitent les CID et faire partie intégrante de l'examen de la diligence (Due Diligence) qui la sous-tend. Conformément à la Circ.-FINMA 08/7 « Outsourcing – banques », la banque continue d'assumer la responsabilité ultime des CID pendant la totalité du cycle de vie des prestations de service externalisées. Les exigences suivantes s'appliquent impérativement aux activités de toute nature impliquant l'accès à de grandes quantités de CID et recouvrent donc aussi bien les prestations de services à grande éechelle (p. ex. prestataires tiers de services IT, support pour l'installation et la maintenance des plate-formes IT développées en externe, hébergement des applications) que les prestations de service étrangères à l'IT (p. ex. externalisation de manifestations pour les clients, etc.).

a) Devoir de diligence en lien avec la confidentialité des CID

55*

Le devoir de diligence en lien avec la confidentialité des CID est constitutif du processus de sélection des prestataires de services externalisés et des fournisseurs de prestations de services à grande échelle. Il convient de définir des critères d'évaluation précis des standards de confidentialité et de sécurité de ces tiers. L'examen portant sur les standards de confidentialité et de sécurité des CID doit être réalisé avant toute convention contractuelle et réitéré périodiquement. Le management suprême doit en outre être informé des modifications déterminantes qui concernent les standards et les solutions en matière de confidentialité appliqués tant en interne que par des tiers.

56*

Le devoir de diligence en relation avec la sécurité et la confidentialité des CID doit être conforté par des informations indépendantes (p. ex. par des normes certifiées ou à l'aide d'audits externes). La banque doit s'assurer que les tiers ayant accès aux CID disposent du savoir-faire et de l'expérience nécessaire dans le domaine de la sécurité et de la protection des données et aient suffisamment de ressources à disposition pour remplir les standards de confidentialité et de sécurité pendant toute la durée contractuelle (y compris à la fin du contrat et durant la phase transitoire).

b) Devoir de diligence en lien avec la confidentialité des CIDS et conventions de prestations de service

57*

Les tiers doivent être informés des standards de sécurité et de confidentialité internes de la banque et s'y conformer en tant qu'exigence minimale. Il convient de préciser dans les conventions de prestations de service la manière dont les tiers satisfont à un éventuel élargissement des standards de sécurité et de confidentialité internes de l'établissement.

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

c) Responsabilité générale

58* Pour chacune des activités externalisées qui comprennent un accès aux CID, la banque doit désigner un ou plusieurs collaborateurs internes qui seront responsables du respect des standards de sécurité et de confidentialité en rapport avec la confidentialité des CID. Ce ou ces collaborateurs sont également chargés d'établir un système de communication avec le prestataire externalisé qui lui ou leur permettent d'annoncer, de surveiller et de documenter tout incident en relation avec les CID intervenant chez le prestataire. La personne responsable en interne doit être en mesure de rapporter en tout temps les conditions et les effets d'un incident grave, en accord avec la stratégie de communication générale (cf. Cm 54 de la présente annexe).

d) Organisation des contrôles et des tests d'efficacité

59* La banque doit savoir et comprendre quels contrôles clés le prestataire externalisé doit réaliser en lien avec la confidentialité des CID. Tous les sujets concernant l'organisation de tels contrôles doivent être définis et abordés avec le prestataire externe. Toutes les prestations de service qui sont fournies par des prestataires externes et présentent des risques en relation avec la confidentialité des CID doivent faire l'objet d'une surveillance constante. Le respect des exigences internes ainsi que l'efficacité des contrôles doivent être contrôlés et évalués.

II. Glossaire

60* Données d'identification du client (*Client Identifying Data*, CID) : données du client qui constituent des données personnelles au sens de l'art. 3 let. a LPD et qui permettent d'identifier le client concerné.

61* Prestations de services à grande échelle : toutes les prestations de service fournies par des tiers qui nécessitent ou permettent potentiellement l'accès à une grande quantité de CID (p. ex. lors de l'implémentation de profils de droits d'accès par les collaborateurs d'un tiers). Un risque lié aux CID peut notamment survenir lors de l'installation d'applications ou de l'implémentation de paramètres locaux (p. ex. droits d'accès), de sauvegarde de données ou de maintenance permanente des systèmes (p. ex. prestataires tiers de services IT, plate-formes IT développées à l'externe). Cela concerne également les travaux internes d'audit et les audits externes. En général, les prestations de service à grande échelle se déploient à long terme.

62* Collaborateurs de tiers : tous les collaborateurs qui travaillent pour des mandataires de la banque (p. ex. mandataire, consultant, auditeur externe, assistance externe, etc.), qui ont accès aux CID et qui ne sont pas des collaborateurs internes.

63* Collaborateurs clés : tous les collaborateurs internes ou externes travaillant dans le domaine IT ou d'autres domaines de l'entreprise qui, en raison de leur profil d'activité et de leurs tâches, disposent dans une large mesure d'un accès privilégié aux CID (p. ex. administrateurs

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

de bases de données, collaborateurs du fichier central).

64*

Incident majeur relatif à la confidentialité des données de clients / fuite d'une grande quantité de données de clients : un incident relatif à la confidentialité des données de clients qui implique une fuite significative de CID (comparée au nombre total des comptes/à la taille totale du portefeuille de clients).

65*

Techniques réversibles de traitement des données :

- Données pseudonymisées (pseudonymisation) : par pseudonymisation, on entend le procédé qui consiste à séparer les données permettant l'identification (p. ex. nom, photo, adresse e-mail, numéro de téléphone) des autres données (p. ex. situation de compte, solvabilité). Des pseudonymes et une règle d'attribution (tableau de concordance) permettent de relier entre deux les deux ensembles de données. Ainsi, des pseudonymes peuvent être créés par un générateur de chiffres aléatoires et attribués, si besoin, à des données personnelles permettant l'identification, grâce à un tableau de concordance.
- Données chiffrées : en pratique, la pseudonymisation peut également être réalisée au moyen d'un procédé de chiffrement. Dans ce cas, le pseudonyme est généré par chiffrement des données personnelles permettant l'identification au moyen d'une clé cryptographique. La ré-identification intervient par déchiffrement à l'aide de la clé secrète.

66*

Techniques irréversibles de traitement des données :

- Données anonymisées : lors de l'anonymisation de données personnelles, tous les éléments permettant l'identification d'une personne sont éliminés ou modifiés de manière irréparable (p. ex. par suppression ou par agrégation), de sorte que les données ne soient plus corrélables à une personne identifiée ou identifiables. En vertu de la définition, ces données ne sont/contiennent plus des CID et ne sont pas soumises à la LPD[24].

III. Exemple de données d'identification des clients

67*

La liste suivante contient des exemples parlants des catégories et éléments de données de clients qu'il faut prendre en compte lors de la définition des données d'identification des clients. Cette liste n'est pas exhaustive.

[24] Cf. PFPDT, annexe sur les exigences minimales qu'un SGPD doit remplir, 5

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

A : Données d'identification directe des clients	B : Données d'identification indirecte des clients	C : Données d'identification potentiellement indirecte des clients
Identification personnelle - Prénom - Nom - Autre(s) prénom(s) - Signature - Nom de jeune fille - Nom de l'époux ou de l'épouse/du ou de la partenaire - Nom de ou des enfants **Identification de l'entreprise** - Nom de l'entreprise - Symbole boursier **Données relatives aux adresses physiques** - Adresses privées - Adresses commerciales - Adresses postales **Données relatives aux adresses électroniques** - Adresses privées (privées, commerciales) - Numéros de téléphone (privés, commerciaux, mobiles, etc.) - Numéros de fax (privés, commerciaux) - ID de réseaux sociaux, y compris les données biométriques comme les photos - Adresses IP - Géolocalisation	**ID personnels/numéros dans les registres publics** - Numéro du passeport - Numéro de la carte d'identité - Numéro d'assurance sociale - Numéro d'attestation militaire - Numéro fiscal - Plaque d'immatriculation - ID Bloomberg - Registre du commerce - Registre foncier - Propriété d'entreprises/de trusts **Identificateurs des clients** - Numéro de client - IBAN/BIC - Numéros de compte - Numéros de coffre-fort - Mot clé (comptes numérotés) - Numéros de contrat - Hypothèques - ID d'utilisateur et mots de passe (p. ex. applications d'e-banking) - ID du portefeuille - Numéros de carte - Champs de texte vierges (comprenant potentiellement des CID) - Documents électroniques (comprenant potentiellement des CID) - Détails bancaires du client auprès de tiers **Données professionnelles clés** - Entreprises - Fonction	**Données relatives à la naissance** - Date de naissance - Lieu de naissance - Nationalité à la naissance (code de nationalité) - Age - Sexe **Données relatives à la famille** - Date du mariage **Mentions personnelles** - Langue (code de langue) - Titres de civilité/universitaires (M^{me}, M., Dr, etc.). - Autres nationalités (code de nationalité) - Situation de famille - Plaques diplomatiques - Loisirs - Adhésions (associations professionnelles, organisations à but caritatif, associations) - Origine de la fortune - Données relatives au cycle de vie **Mentions personnelles relatives à la domiciliation** - Pays de résidence (code de pays) - Pays du domicile fiscal **Profil professionnel** - Qualifications professionnelles - Profession, fonction - Date de la fondation / liquidation / des introductions en bourse de l'entreprise **Identificateurs de l'entreprise** - Désignation de la fonction de management dans une société anonyme, p. ex. CRO - Actionnaire principal (J/N)

Annexe 43*

Traitement des données électroniques de clients~~Comparaison entre la Circ.-FINMA et les standards minimaux du Comité de Bâle~~

A : Données d'identification directe des clients	B : Données d'identification indirecte des clients	C : Données d'identification potentiellement indirecte des clients
		Mentions relatives à l'entreprise ne permettant pas son identification - Forme juridique de l'entreprise - Année de la fondation - Branche (code NOGA) - Noms des concurrents **Données d'identification de la relation** - Segment de clientèle - Nom/sigle du contact interne du client - Monnaie du compte - Succursale - Performance du client **Besoins des clients et utilisation du produit** - Comportement/type de placement - Phase du cycle de vie - Stratégie de l'entreprise - Données relatives aux produits - Notation financière - Données relatives aux transaction / mouvements sans CID - Positions du portefeuille - Situation du compte

Liste des modifications

La présente circulaire est modifiée comme suit :

Modification du 1er juin 2012 entrant en vigueur le 1er janvier 2013.

Cm modifié	84

Dans toute la circulaire, les renvois à l'ordonnance sur les fonds propres (OFR ; RS 952.03) ont été adaptés à la version de ladite ordonnance qui entre en vigueur au 1er janvier 2013.

Modifications du xx.yy.2013 entrant en vigueur le 1er janvier 2015 (à l'exception du Cm 116 qui entre en vigueur le 1er janvier 2014).

Nouveaux Cm	2.1, 116, 117 à 136, 137
Cm modifiés	1, 29, 50, 53, 71, 79
Cm abrogés	20 à 22, 28, 30 à 44, 64

Les annexes de la circulaire sont modifiées comme suit :

Modifications du xx.yy.2013 entrant en vigueur le 1er janvier 2015.

Modifiée / Nouvelle	annexe 3
Abrogées	annexes 1 et 4

La numérotation des annexes a, par ailleurs, été adaptée.