
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 :	1 ^{er} janvier 2009
Dernière modification :	31 octobre 2019 [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, 4 ^{bis} al. 2 OB art. 12 LBVM art. 10 al. 2 let. a OBVM art. 19 al. 3, 20 al. 1, 29 OFR art. 2, 89 à 94 Oém-FINMA art. 5 ss
Annexe 1 :	Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR
Annexe 2 :	Vue d'ensemble pour la catégorisation des types d'événements
Annexe 3 :	Traitement des données électroniques de clients

Destinataires		
<input checked="" type="checkbox"/>	Banques	LB
<input checked="" type="checkbox"/>	Groupes et congl. financiers	
	Autres intermédiaires	
	Assureurs	LSA
	Groupes et congl. d'assur.	
	Intermédiaires d'assur.	
<input checked="" type="checkbox"/>	Négociants en valeurs mob.	LBVM
	Plates-formes de négociation	
	Contreparties centrales	LIMF
	Dépositaires centraux	
	Référentiels centraux	
	Systèmes de paiement	
	Participants	
	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	

abrogé

I. Objet	Cm	1
II. Définition	Cm	2–2.1
III. Exigences de fonds propres	Cm	3–116
A. Approche de l'indicateur de base (BIA, art. 92 OFR)	Cm	3–22
B. Approche standard (AS, art. 93 OFR)	Cm	23–44
a) Mécanisme	Cm	23–27
b) Exigences générales (art. 93 al. 3 OFR)	Cm	28–29
c) Abrogé	Cm	30–44
C. Approches spécifiques aux établissements (AMA, art. 94 OFR)	Cm	45–107
a) Autorisation	Cm	45–49
b) Exigences qualitatives supplémentaires	Cm	50–68
c) Exigences quantitatives générales	Cm	69–75
d) Données internes relatives aux pertes (art. 94 al. 2 OFR)	Cm	76–85
e) Données externes relatives aux pertes (art. 94 al. 2 OFR)	Cm	86–88
f) Analyse de scénarios (art. 94 al. 2 OFR)	Cm	89–91
g) Environnement d'affaires et système de contrôle interne (art. 94 al. 2 OFR)	Cm	92–97
h) Atténuation du risque par des assurances	Cm	98–107
D. Utilisation partielle d'approches	Cm	108–114
E. Ajustements des exigences de fonds propres (art. 45 OFR)	Cm	115
F. Fonds propres minimaux et plancher (<i>floor</i>)	Cm	116
IV. Exigences qualitatives concernant la gestion des risques opérationnels	Cm	117–138
A. Principe de proportionnalité	Cm	117–118
B. Exigences qualitatives de base	Cm	119–134
a) Principe 1 : catégorisation et classification des risques opérationnels	Cm	121–124

b)	abrogé	Cm	125-127
c)	Principe 2 : identification, limitation et surveillance	Cm	128–130
d)	Principe 3 : établissement de rapports internes et externes	Cm	131–134
e)	Principe 4 : infrastructure technologique	Cm	135–135.12
f)	Principe 5 : continuité en cas d'interruption de l'activité	Cm	136
g)	Principe 6 : maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique	Cm	136.1
h)	Principe 7 : risques liés aux activités de service transfrontières	Cm	136.2–136.5
C.	Exigences qualitatives spécifiques au risque	Cm	137–138
V.	Audit et évaluation par les sociétés d'audit	Cm	139

abrogé

I. Objet

La présente circulaire concrétise les art. 89 à 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. 12 OB et des art. 19 à 20 OBVM. Dans le domaine quantitatif, 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.

1*

II. Définition

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 et de *compliance*, dans la mesure où ils représentent une perte financière directe, c.-à-d. y compris les amendes d'autorités de surveillance ou d'autres autorités.

2*

Abrogé

2.1*

III. Exigences de fonds propres

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

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.

3

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 résultat 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 1^{er} juillet 2005 au 30 juin 2006, 1^{er} juillet 2006 au 30 juin 2007 et 1^{er} juillet 2007 au 30 juin 2008.

4

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

5

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).

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

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 125 ss Circ.-FINMA 15/1 « Comptabilité – banques » : 9*

- résultat brut des opérations d'intérêts (Cm 131 Circ.-FINMA 15/1 « Comptabilité – banques ») ; 10*
- résultat des opérations de commissions et des prestations de service² (Cm 139 Circ.-FINMA 15/1 « Comptabilité – banques ») ; 11*
- résultat des opérations de négoce et de l'option de la juste valeur (Cm 140 Circ.-FINMA 15/1 « Comptabilité – banques ») ; 12*
- résultat des participations non consolidées (Cm 143 Circ.-FINMA 15/1 « Comptabilité – banques ») ; et 13*
- résultat des immeubles (Cm 144 Circ.-FINMA 15/1 « 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 historiques 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 la FINMA. 16

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

² La prise en considération des charges de commissions selon le Cm 138 Circ.-FINMA 15/1 « Comptabilité – banques » est soumise aux restrictions du Cm 18.

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 mandante 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

Abrogé 20*-22*

B. Approche standard (AS, 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 à 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 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). 24

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,

• $G_{i,j}$ 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)	
Abrogé	28*
Chaque banque doit définir, conformément à l'annexe 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) Abrogé	
Abrogé	30*-44*
C. Approches spécifiques aux établissements (AMA, art. 94 OFR)	
a) Autorisation	
Les approches spécifiques aux établissements (<i>advanced measurement approaches</i> , 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 FINMA.	46
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.	47
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.	48
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.	49

b) Exigences qualitatives supplémentaires

Les banques qui utilisent une approche spécifique à l'établissement doivent satisfaire aux exigences qualitatives de base selon le chapitre IV.B.	50*
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.	51
L'organe responsable de la haute direction, la surveillance et le contrôle doit être impliqué de manière active dans la surveillance de l'approche.	52
La direction doit être familiarisée avec le concept de base de l'approche et être à même d'exercer ses fonctions de surveillance en la matière.	53*
La banque dispose pour la gestion des risques opérationnels d'un système conceptionnel solidement conçu, fiable et mis en œuvre avec intégrité.	54
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.	55
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 :	56
<ul style="list-style-type: none">• l'établissement de principes et de procédures pour la gestion et le contrôle des risques opérationnels à l'échelle de la banque ;	57
<ul style="list-style-type: none">• la conception et l'application de la méthodologie de quantification des risques opérationnels propre à l'établissement ;	58
<ul style="list-style-type: none">• la conception et la mise en place d'un système d'annonce des risques opérationnels ; et	59
<ul style="list-style-type: none">• 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
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
<ul style="list-style-type: none">• vérification du bon fonctionnement des processus internes de validation ; et	67
<ul style="list-style-type: none">• 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 avec la société d'audit.	69
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.	70
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 classer les événements générateurs de pertes conformément à l'annexe 2.	71*

³ Voir note 1.

Des fonds propres exigibles sont déterminées tant pour les pertes attendues qu'inattendues. La FINMA peut toutefois accorder des allègements à cet égard si la banque a constitué des provisions adéquates pour pertes futures attendues.	72
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.	73
Chaque approche doit présenter certaines caractéristiques de base. A leur nombre figure notamment la satisfaction des exigences relatives à l'intégration :	74
<ul style="list-style-type: none">• de données internes relatives aux pertes (Cm 76 à 85) ;• de données externes pertinentes relatives aux pertes (Cm 86 à 88) ;• de procédures d'analyses des scénarios (Cm 89 à 91) ; et• de facteurs de l'environnement d'affaires et du système de contrôle interne (Cm 92 à 97).	
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.	75
d) Données internes relatives aux pertes (art. 94 al. 2 OFR)	
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.	76
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 période 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.	77
Le processus de création d'une base de données interne pour les pertes opérationnelles doit satisfaire aux exigences suivantes :	78
<ul style="list-style-type: none">• 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 2.	79*

Pour pouvoir procéder à cette classification, elle doit disposer de critères objectifs bien documentés.

- 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. 80
- 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 supérieurs ou égaux à un montant brut de 1 million de francs suisses, des explications relatives à la cause de la perte doivent être consignées. 81
- 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. 82

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. 83

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 à 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*). 84*

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. 85

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

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. 86

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. 87

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. 88

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

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

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. 90

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. 91

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

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). 92

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 :	93
<ul style="list-style-type: none">• 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.	94
<ul style="list-style-type: none">• 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.	95
<ul style="list-style-type: none">• 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.	96
<ul style="list-style-type: none">• 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.	97
h) Atténuation du risque par des assurances	
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.	98
Les possibilités de réduire les exigences de fonds propres sont liées au respect des conditions suivantes :	99
<ul style="list-style-type: none">• 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.	100
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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	102

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.

- 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 à 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 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 apparaît 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 suivant s'applique en vertu du maintien du « régime de *floor* » publié par le Comité de Bâle⁴ : 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 évaluer 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 définit, en application de l'art. 47 OFR, la manière de procéder au calcul approximatif adéquat des exigences théoriques selon Bâle I. Pour les risques opérationnels, elle se réfère à l'approche standard selon l'art. 93 OFR. 116*

IV. Exigences qualitatives concernant la gestion des risques opérationnels

A. Principe de proportionnalité

Les exigences présentées dans ce chapitre s'appliquent en principe à tous les destinataires de cette circulaire. Elles doivent cependant être implémentées au cas par cas, en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement. Le Cm 117*

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

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

119 énumère les chiffres marginaux pour lesquels les petits établissements sont totalement exemptés d'application.

Les petits établissements au sens du Cm 117 sont les banques et les négociants en valeurs mobilières des catégories⁶ 4 et 5 de la FINMA. La FINMA peut ordonner des allègements ou des renforcements au cas par cas. 118*

B. Exigences qualitatives de base

Les petits établissements au sens des Cm 117 et 118 sont exemptés de l'application des Cm 129 et 132 à 134. 119*

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).⁷ 120*

a) Principe 1 : catégorisation et classification des risques opérationnels

Les risques opérationnels doivent être catégorisés⁸ de façon uniforme afin d'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. 121*

La classification uniforme des risques opérationnels s'effectue sur la base de la catégorisation des risques opérationnels selon le Cm 121 et inclut aussi bien une évaluation des risques inhérents⁹ que des risques résiduels¹⁰. La classification peut être réalisée sur la base de l'évaluation tant qualitative que quantitative. La classification sert notamment aussi à la détermination des risques de grande envergure au sens du Cm 137. 122*

Abrogé 123*-124*

b) Abrogé

Abrogé 125*-127*

c) Principe 2 : identification, limitation et surveillance

Une identification des risques efficace, qui constitue la base de la limitation et de la surveillance des risques opérationnels, prend en compte aussi bien des facteurs internes¹¹ qu'externes¹². Elle inclut au moins des évaluations de risques et de contrôles ainsi que les résultats de la révision. 128*

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

⁷ www.bis.org/publ/bcbs195.pdf

⁸ Cette catégorisation uniforme peut être réalisée sur le modèle de l'annexe 2 de la présente circulaire ou au moyen d'une terminologie ou taxonomie interne.

⁹ Cf. annexe 3, Cm 59

¹⁰ Cf. annexe 3, Cm 60

¹¹ Par exemple structure de l'entreprise, nature des activités, qualifications des collaborateurs, changements sur le plan organisationnel et fluctuation de l'effectif d'une banque.

¹² Par exemple modifications de l'environnement élargi et de la branche ainsi qu'avancées technologiques.

En fonction des activités commerciales spécifiques à l'établissement ainsi que de la nature, de l'ampleur, de la complexité et de la teneur en risque de ces dernières, le recours à d'autres instruments et méthodes doit être envisagé et, le cas échéant, retenu :	129*
a. la collecte et l'analyse des données internes relatives aux pertes ;	
b. la collecte et l'analyse des événements externes liés à des risques opérationnels ;	
c. l'analyse des rapports entre risques, processus et contrôles ;	
d. les indicateurs de risque et de performance pour la surveillance des risques opérationnels et les indicateurs concernant l'efficacité du système de contrôle interne ;	
e. les analyses de scénarios ;	
f. l'estimation du potentiel de perte ;	
g. les analyses comparatives ¹³ .	
La limitation et la surveillance sont effectuées par les unités organisationnelles prévues à cet effet à l'aide des instruments, structures, approches, etc. qui ont été définis dans le cadre de la gestion des risques à l'échelle de l'établissement selon la Circ.-FINMA 17/1.	130*
d) Principe 3 : établissement de rapports internes et externes	
Abrogé	131*
L'établissement de rapports internes sur les risques opérationnels doit intégrer des données concernant la finance, l'exploitation et la <i>compliance</i> , mais aussi les principales informations externes pertinentes pour le risque au sujet des événements et des conditions. Le rapport sur les risques opérationnels doit au moins comprendre les points suivants et présenter leurs répercussions possibles sur l'établissement et le capital propre requis pour les risques opérationnels :	132*
a. les déviations matérielles à la tolérance au risque de l'établissement définie sur la base des risques inhérents et résiduels ainsi que les dépassements des limites de risque définies dans ce cadre ;	132.1*
b. les détails sur les événements internes matériels liés aux risques opérationnels et/ou les pertes ;	132.2*
c. les informations relatives aux événements externes susceptibles d'être pertinents pour l'établissement ainsi que les risques potentiels et leurs possibles répercussions sur l'établissement.	132.3*

¹³ 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.

Un établissement doit disposer d'une politique de déclaration formelle, approuvée par l'organe responsable de la direction supérieure, d'où il ressort la manière dont la banque déclare ses risques opérationnels et les processus de contrôle qu'il faut appliquer en matière de déclaration. 133*

Les informations que les établissements 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. 134*

e) Principe 4 : infrastructure technologique¹⁴

La direction doit documenter sous une forme appropriée la gestion des risques liés à l'infrastructure technologique en adéquation avec la stratégie IT et la tolérance au risque définie tout en tenant compte des aspects pertinents spécifiques pour l'établissement des standards internationalement reconnus. 135*

La direction s'assure que soient couverts par la gestion des risques liés à l'infrastructure technologique les aspects suivants au moins : 135.1*

a. vue d'ensemble actualisée des principaux éléments de l'infrastructure de réseau et inventaire de toutes les applications critiques, de l'infrastructure IT liée et des interfaces avec des tiers, 135.2*

b. définition claire des rôles, tâches et responsabilités en relation avec les applications critiques ainsi que de l'infrastructure IT liée et des données et processus critiques et/ou sensibles, 135.3*

c. processus systématique pour l'identification et l'évaluation des risques IT dans le cadre de l'examen de diligence (*Due Diligence*), en particulier lors d'acquisition respectivement d'externalisation dans le domaine IT ainsi que pour la surveillance des conventions de prestations, 135.4*

d. mesures visant à renforcer la prise de conscience par les collaborateurs de leur responsabilité concernant la réduction des risques IT ainsi que le respect et le renforcement de la sécurité IT. 135.5*

La direction doit en outre documenter sous une forme appropriée la gestion des cyber-risques¹⁵. Celle-ci doit au minimum couvrir les aspects suivants et garantir une mise en œuvre efficace grâce à des processus appropriés ainsi qu'une définition claire des tâches, rôles et responsabilités : 135.6*

¹⁴ 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.

¹⁵ Risques opérationnels en relation avec les pertes éventuelles causées par des cyberattaques.

- a. identification des risques potentiels de cyberattaques¹⁶ spécifiques à l'établissement, notamment en ce qui concerne les données et systèmes IT critiques et/ou sensibles, 135.7*
- b. protection des processus opérationnels et de l'infrastructure technologique contre les cyberattaques, notamment sous l'angle de la confidentialité, de l'intégrité et de la disponibilité des données et des systèmes IT critiques et/ou sensibles, 135.8*
- c. identification et désignation rapides des cyberattaques sur la base d'un processus de surveillance systématique de l'infrastructure technologique, 135.9*
- d. réaction aux cyberattaques grâce à des mesures immédiates et ciblées et, dans les cas matériels, maintien de l'activité opérationnelle normale en concertation avec le BCM, et 135.10*
- e. garantie d'un rétablissement rapide de la marche normale des affaires après des cyberattaques, grâce à des mesures appropriées. 135.11*

La direction ordonne régulièrement des analyses de vulnérabilité¹⁷ et des tests d'intrusion (*penetration testings*)¹⁸, afin de protéger les données et systèmes IT critiques et/ou sensibles contre les cyberattaques. Ceux-ci doivent être confiés à du personnel qualifié disposant des ressources appropriées. 135.12*

f) Principe 5 : continuité en cas d'interruption de l'activité

La direction doit disposer de plans de maintien des affaires de l'établissement qui garantissent la continuité des activités et la délimitation des dommages en cas d'interruption grave de l'activité.¹⁹ 136*

g) Principe 6 : maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique

Dans le cadre de leur plan d'urgence, les banques d'importance systémique prennent les mesures requises pour que leurs fonctions d'importance systémique puissent être poursuivies sans interruption (art. 9 al. 2 let. d LB en rel. avec les art. 60 ss OB). Elles identifient les requis pour la poursuite des fonctions d'importance systémique en cas de liquidation, d'assainissement ou de restructuration (« prestations critiques ») et prennent les mesures nécessaires à leur poursuite. Elles tiennent compte à cet égard des prescriptions des organismes édictant les standards internationaux. 136.1*

¹⁶ Il s'agit d'attaques en provenance d'Internet et de réseaux comparables qui visent l'intégrité, la disponibilité et la confidentialité de l'infrastructure technologique, notamment en ce qui concerne les données et systèmes IT critiques et/ou sensibles.

¹⁷ Analyse visant à identifier les points faibles actuels des logiciels ainsi que les failles de sécurité de l'infrastructure IT par rapport aux cyberattaques.

¹⁸ Test ciblé et utilisation des points faibles des logiciels et des failles de sécurité de l'infrastructure technologique afin d'accéder sans autorisation à cette dernière.

¹⁹ Cf. les chiffres des recommandations de l'ASB en matière de *Business Continuity Management* (BCM) reconnus comme standards minimaux.

h) Principe 7 : risques liés aux activités de service transfrontières

Quand des établissements ou leurs filiales fournissent des services financiers ou de distribution de produits financiers dans le cadre d'opérations transfrontières, les risques résultant d'une application des législations étrangères (droit fiscal, droit pénal, législation en matière de blanchiment d'argent, etc.) doivent également être identifiés, limités et contrôlés de façon appropriée. En tant qu'autorité de surveillance, la FINMA s'attend en particulier à ce que les banques respectent le droit étranger de la surveillance. 136.2*

Les établissements soumettent leurs activités de services financiers transfrontières ainsi que la distribution transfrontière de produits financiers à une analyse approfondie des conditions cadre juridiques et des risques correspondants. Sur la base de cette analyse, les établissements prennent les mesures stratégiques et organisationnelles nécessaires à l'élimination et à la minimisation des risques et les adaptent au fur et à mesure à l'évolution de la situation. Ils possèdent notamment les connaissances spécialisées spécifiques aux pays requises, définissent des modèles de prestations spécifiques aux pays desservis, forment les collaborateurs et garantissent le respect des prescriptions grâce à des mesures organisationnelles, des directives et des modèles de rémunération et de sanction correspondants. 136.3*

Les risques générés par les gérants de fortune indépendants, les intermédiaires et autres prestataires doivent également être pris en compte. En conséquence, ces partenaires doivent être choisis et instruits avec soin. 136.4*

Ce principe s'applique également aux cas dans lesquels une filiale, une succursale ou une entité similaire d'un établissement financier suisse domiciliée à l'étranger offre des services transfrontières à des clients. 136.5*

C. Exigences qualitatives spécifiques au risque

Les risques opérationnels spécifiques de grande envergure nécessitent un pilotage et un contrôle plus complets et plus intensifs que ceux prescrits dans le cadre des exigences qualitatives de base. En fonction de la situation, la direction doit, pour ce faire, définir et mettre en œuvre des mesures spécifiques au risque complémentaires ou renforcer les mesures existantes. 137*

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. 138*

V. Audit et évaluation par les sociétés d'audit

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. 139*

Annexe 1

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

I. Vue d'ensemble

1

1 ^{er} niveau	2 ^e 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 (<i>Initial Public Offerings</i>), placements privés sur le marché secondaire
	Collectivités publiques	
	Banques d'affaires (<i>merchant banking</i>)	
	Prestations de conseil	
Négoce	Négoce pour compte de clients	Emprunts, actions, change, matières premières, crédits, dérivés, financement (<i>funding</i>), négoce pour compte propre, prêts et mises en pension de titres (<i>repos</i>), courtage (pour des investisseurs n'appartenant pas à la clientèle de détail), courtage de premier rang (<i>prime brokerage</i>)
	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, <i>leasing</i> , octrois de crédits, garanties et cautionnements, effets de change
Trafic des paiements/règlement de titres ²⁰	Clientèle externe	Opérations de paiement, compensation et règlement d'opérations sur titres pour des tiers
Affaires de dépôt et dépôts fiduciaires	Garde de titres (<i>custody</i>)	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

²⁰ 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.

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

	Service de fiducie aux entreprises (<i>corporate trust</i>)	
Gestion d'actifs institutionnelle	Gestion d'actifs discrétionnaire	Gestion centralisée, segmentée, relative à la clientèle de détail, institutionnelle, fermée, ouverte, <i>private equity</i>
	Gestion d'actifs non discrétionnaire	Gestion centralisée, segmentée, relative à la clientèle de détail, individuelle, privée, 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 (1^{er} 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

Annexe 1



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

- | | |
|---|----|
| 7. La banque doit disposer de procédures lui permettant de classier de nouvelles activités ou de nouveaux produits. | 8 |
| 8. La responsabilité des principes de classification incombe à la direction. Ceux-ci sont soumis à l'approbation de l'organe responsable de la haute direction, la surveillance et le contrôle. | 9* |
| 9. Les procédures de classification seront vérifiées régulièrement par la société d'audit. | 10 |

abrogé

Vue d'ensemble pour la catégorisation 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	<p>Transactions non notifiées (intentionnellement)</p> <p>Transactions non autorisées (avec préjudice financier)</p> <p>Saisie (intentionnellement) erronée de positions</p>
		Vol et fraude	<p>Fraude, fraude au crédit, dépôts sans valeur</p> <p>Vol, extorsion et chantage, abus de confiance, brigandage</p> <p>Détournement de biens</p> <p>Destruction malveillante de biens</p> <p>Contrefaçons</p> <p>Falsification de chèques</p> <p>Contrebande</p> <p>Accès non autorisé à des comptes de tiers</p> <p>Délits fiscaux</p> <p>Corruption</p> <p>Délits d'initié (pas pour le compte de l'entreprise)</p>
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	Vol et fraude	<p>Vol, brigandage</p> <p>Contrefaçons</p> <p>Falsification de chèques</p>

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

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
	d'une partie interne à l'entreprise)	Sécurité des systèmes informatiques	<p>Dommmages dus au piratage informatique</p> <p>Accès non autorisé à des informations (avec préjudice financier)</p>
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	<p>Responsabilité civile</p> <p>Infractions aux dispositions relatives à la sécurité et à la santé du personnel</p> <p>Indemnisations ou dommages-intérêts versés au personnel</p>
		Discrimination	Dommmages-intérêts versés au titre d'actions en discrimination

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

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
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	<p>Violation du devoir fiduciaire, non-respect de directives</p> <p>Problèmes posés par la conformité et la diffusion d'informations (règles du <i>Know-your-Customer</i>, etc.)</p> <p>Violation du devoir d'informer la clientèle</p> <p>Violation du secret professionnel du banquier ou de dispositions relatives à la protection des données</p> <p>Pratiques de vente agressives</p> <p>Création inappropriée de commissions et de courtage</p> <p>Utilisation abusive d'informations confidentielles</p> <p>Responsabilité du prêteur</p>
		Pratiques commerciales ou sur le marché incorrectes	<p>Violation de dispositions antitrust</p> <p>Pratiques de place illicites</p> <p>Manipulation du marché</p> <p>Délits d'initié (pour le compte de l'entreprise)</p> <p>Activités commerciales sans autorisation correspondante</p> <p>Blanchiment d'argent</p>

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

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
		Problèmes avec des produits	Problèmes liés à des produits (absence de pouvoirs, etc.) Fautes en matière de modèles
		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
Dompage 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.

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

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
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	<p>Problèmes de communication</p> <p>Erreurs lors de la saisie ou dans le suivi des données</p> <p>Dépassement d'un délai</p> <p>Non-exécution d'une tâche</p> <p>Erreurs dans l'utilisation d'un modèle ou d'un système</p> <p>Erreurs comptables ou affectation à une fausse unité</p> <p>Livraison erronée ou non effectuée</p> <p>Gestion inappropriée d'instruments de couverture</p> <p>Erreurs dans la gestion des données de référence</p> <p>Erreurs concernant d'autres tâches</p>
		Surveillance et annonces	<p>Non-respect de devoirs d'annoncer</p> <p>Rapports inadéquats remis à des externes (ayant entraîné une perte)</p>
		Admission de clientèle et documentation	Non-respect des règles internes et externes en la matière

Annexe 2

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

Catégorie d'événement générateur de perte (niveau 1)	Définition	Sous-catégories (niveau 2)	Exemple d'activités (niveau 3)
		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

Traitement des données électroniques de clients

La présente annexe énonce les principes de bonne gestion des risques en lien avec la confidentialité des données électroniques des personnes physiques (« particuliers »²¹) 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 de grandes quantités de données de clients du fait de l'utilisation de systèmes électroniques. Ils n'abordent que de manière marginale les réflexions sur la sécurité des données physiques ou les questions d'intégrité et de disponibilité des données. Les dispositions juridiques pertinentes ne trouvent pas seulement leur source dans le droit de la surveillance²², mais aussi dans la législation relative à la protection des données²³ et dans le droit civil.

1*

Les petites²⁴ banques sont exemptées de la mise en œuvre des chiffres marginaux suivants :

2*

- Cm 15 et 17 à 19, ainsi que 22 du principe 3 ;
- tous les chiffres marginaux des principes 4 à 6 ;
- Cm 41 du principe 7.

Les établissements selon les art. 47a à 47e OFR ainsi que les établissements au sens de l'art. 1b LB peuvent se limiter à la mise en œuvre des exigences du Cm 3 de l'annexe 3. L'exigence du Cm 3 doit être mise en œuvre au cas par cas, en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement.

2.1*

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

A. Principe 1 : gouvernance

Les risques en lien avec la confidentialité des données de clients sont systématiquement identifiés, limités et surveillés. A cet effet, l'organe responsable de la haute direction surveille la direction pour s'assurer d'une implémentation efficace des mesures destinées à garantir la confidentialité des données des clients. La direction mandate une unité indépendante assurant la fonction de contrôle pour établir et préserver les conditions-cadre garantissant la confidentialité des données des clients.

3*

a) Indépendance et responsabilité

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.

4*

²¹ Par « particuliers », on entend aussi les relations commerciales dans lesquelles la personne physique établit une relation commerciale avec la banque en passant par une personne morale (p. ex. en qualité d'ayant droit économique d'une société de siège, d'une société de domicile, d'une fondation) ou par un trust.

²² Notamment art. 3 et 47 LB ainsi qu'art. 12 OB ; art. 10 et 43 LBVM ainsi qu'art. 19 s. OBVM.

²³ Notamment art. 7 LPD ainsi qu'art. 8 ss OLPD (cf. également à ce sujet les guides du PFPDT).

²⁴ Cf. Cm 118

Traitement des données électroniques de clients

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, puis approuvées par l'organe responsable de la haute direction. La direction informe régulièrement l'organe responsable de la direction supérieure de l'efficacité des contrôles introduits. 5*

b) Règles, processus et systèmes

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 est présumé existant. Ce concept cadre doit être mis en œuvre de manière cohérente dans l'ensemble des domaines fonctionnels et des unités qui ont accès aux données des clients ou traitent ces dernières. 6*

Des mesures tenant compte de la tolérance au risque définie par la banque ainsi que la périodicité avec laquelle elles seront mises en œuvre sont à définir par écrit, de manière compréhensible et contraignante. 7*

L'implémentation et le respect du concept cadre relatif à la confidentialité des données des clients doivent être soumis à la surveillance de l'organe responsable de la haute direction et être garantis par des contrôles réguliers de l'unité compétente pour la confidentialité et la sécurité des données. 8*

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

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 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*). 9*

a) Catégories de données de clients et définition des CID

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 indirectes 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. 11*

Traitement des données électroniques de clients

b) Classification des CID et niveaux de confidentialité

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*

c) Responsabilité des CID

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. 13*

Les unités responsables des CID (*Data Owners*) sont chargées de l'implémentation des directives de classification des données ainsi que de la justification et de la documentation des exceptions. 14*

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

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*. 15*

a) Lieu de stockage et accès aux données en général

Un inventaire des applications et de l'infrastructure y afférente qui renferment ou traitent des CID doit être disponible et actualisé au fur et à mesure. L'actualisation de l'inventaire, notamment en cas de changements structurels (par ex. nouveaux sites géographiques ou renouvellement de l'infrastructure technique), doit être entreprise dans les meilleurs délais. Des mises à jour régulières sont nécessaires pour les changements d'importance moindre. 16*

On part du principe que la granularité de l'inventaire permet à la banque d'établir : 17*

- 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) ; 18*
- 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). 19*

Traitement des données électroniques de clients

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

Lorsque les CID sont stockées hors de Suisse ou qu'elles font l'objet d'un accès depuis l'étranger, les risques accrus qui en résultent sur le plan de la protection des données des clients doivent être limités de manière appropriée.²⁵ Les CID doivent être protégées de manière adéquate (p. ex. anonymisation, chiffrement ou pseudonymisation). 20*

c) Principe du *need to know*

Les personnes ne doivent avoir accès qu'aux informations et aux fonctionnalités nécessaires à l'exercice de leurs tâches. 21*

d) Autorisation d'accès

La banque doit disposer d'un système d'autorisation fondé sur les fonctions et les rôles qui régit sans équivoque les droits d'accès des collaborateurs et des tiers au CID. Ces droits d'accès doivent faire l'objet de confirmation régulière afin de garantir que seules les personnes bénéficiant d'une autorisation valable à la date concernée aient accès aux CID. 22*

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

Les normes de sécurité liées à 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'évolution 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. 23*

a) Normes de sécurité

Les normes de sécurité doivent être en adéquation avec la taille de la banque et le degré de complexité de son architecture IT. 24*

b) Normes de sécurité et pratique du marché

Les normes de sécurité sont une partie intégrante inamovible du concept cadre garantissant la confidentialité des données des clients. Elles doivent être confrontées 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. 25*

²⁵ Il faut en outre respecter les dispositions déterminantes du droit de la protection des données, comme celles de l'art. 6 LPD.

Traitement des données électroniques de clients

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

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

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

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

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

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 (hautement privilégiés (par ex. administrateurs système) et usagers disposant d'un accès fonctionnel à des grandes quantités de CID (« collaborateurs clés »), auxquels il convient de prêter une attention particulière.

a) Sélection soigneuse des collaborateurs

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 fixer contractuellement les modalités selon lesquelles les collaborateurs sont sélectionnés par des tiers ou désignés par les entreprises tierces qui, sur mandat de la banque, peuvent accéder aux CID, afin que tous les collaborateurs soient sélectionnés avec soin dans le cadre d'un processus comparable.

b) Formations ciblées des collaborateurs

Les collaborateurs internes et externes doivent être sensibilisés aux questions relatives à la sécurité des données des clients dans le cadre de formations ciblées.

c) Exigences de sécurité

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

Traitement des données électroniques de clients

utilisateurs IT (hautement) privilégiés et usagers disposant d'un accès fonctionnel²⁶ à une grande quantité de CID (« collaborateurs clés »).

d) Liste des collaborateurs clés

En complément des exigences générales applicables aux autorisations d'accès pour les collaborateurs et pour les tiers (voir Cm 22), la banque est tenue de tenir et d'actualiser au fur et à mesure une liste des noms de tous les utilisateurs IT (hautement) privilégiés et usagers, internes et externes, qui ont un accès à des grandes quantités de CID²⁷ et/ou auxquels des responsabilités en matière de contrôle et de surveillance de la confidentialité des données des clients ont été transférées. 34*

Des dispositifs tels que la tenue de fichiers-journaux doivent être introduits afin de permettre l'identification des utilisateurs qui ont accès à une grande quantité de CID. 35*

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

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 processus structuré. Ce processus doit comprendre les scénarios de risque²⁸ en relation avec la confidentialité des CID qui sont pertinents pour la banque et la définition des contrôles clés correspondants. L'adéquation du catalogue des contrôles clés en relation avec la confidentialité des données, qui est destiné à garantir la protection des CID, doit être vérifiée en permanence et, le cas échéant, conduire à des adaptations. 36*

a) Processus d'évaluation du risque

L'évaluation du risque inhérent à la confidentialité des CID et du risque résiduel doit intervenir sur la base d'un processus structuré et en impliquant les utilisateurs finaux ainsi que les fonctions informatiques et de contrôle. 37*

b) Scénarios de risque et contrôles clés²⁹

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. 38*

²⁶ En cas de droits d'accès étendus, par ex. consultation et extraction/migration d'une grande quantité de CID.

²⁷ Les consultations individuelles relevant de droits d'accès restreints (par ex. par les collaborateurs aux guichets) n'entrent pas dans la définition de l'accès à de grandes quantités de CID.

²⁸ 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.

²⁹ 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).

Traitement des données électroniques de clients

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

Les risques identifiés doivent être surveillés et limités de manière appropriée. Ce principe vaut en particulier pour les activités de traitement des données au cours desquelles de grandes quantités de CID doivent être modifiées ou migrées.³⁰ 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.

39*

a) Environnement de production, traitement des données portant sur une grande quantité de CID

Le traitement des données qui, dans l'environnement productif, est réalisé avec une grande quantité de CID qui ne sont pas anonymisées, chiffrées, ni pseudonymisées, doit être soumis à des procédures appropriées (p. ex. principe du double contrôle ou fichiers journaux), intégrant l'information de l'unité compétente pour la sécurité et la confidentialité des données.

40*

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

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.

41*

Si un établissement n'applique aucune méthode d'anonymisation, de pseudonymisation ou de chiffrement (travail « en clair ») lors du développement, de la transformation et de la migration de systèmes (par ex. lors de la création de données tests ou lors de l'enregistrement intermédiaire de données durant leur migration), il doit respecter lors de ces activités les consignes énoncées au Cm 40.

41.1*

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

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 ainsi que les résultats des audits et des contrôles 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.

42*

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

Il faut formaliser un processus clairement défini d'identification des incidents en rapport avec la confidentialité ainsi que la réaction qu'elle implique et communiquer ce dernier à toutes les parties concernées au sein de l'établissement.

43*

³⁰ 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.

Traitement des données électroniques de clients

b) Annonce

Il faut que le risque lié à la violation de la confidentialité des CID et les signalements de *compliance* s'y rapportant soient présentés de manière adéquate dans les rapports internes ou que la saisie et la remontée aux organes appropriés soient garanties si le secret lié à ces événements l'exige. 44*

c) Amélioration permanente du cadre garantissant la confidentialité des CID

Le concept cadre destiné à garantir la confidentialité des CID (Cm 6, 7 et 8) et les standards de sécurité (Cm 24) doivent faire l'objet de contrôles périodiques. Les incidents, les exceptions ainsi que les résultats des audits et des contrôles doivent contribuer à l'amélioration permanente de ce concept cadre. 45*

d) Communication externe

La banque doit disposer d'une stratégie de communication claire en cas d'incidents graves en 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. 46*

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

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 échelle (p. ex. prestataires tiers de services IT, support pour l'installation et la maintenance des plateformes 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.). 47*

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

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. 48*

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

Les tiers doivent être informés des standards de sécurité et de confidentialité internes de la banque et de leurs éventuels élargissements et s'y conformer en tant qu'exigence minimale. 49*

Traitement des données électroniques de clients

c) Responsabilité générale

Pour chacune des activités externalisées qui comprennent un accès aux CID, la banque doit désigner au moins un collaborateur interne qui sera responsable du respect des standards de sécurité et de confidentialité en rapport avec la confidentialité des CID. 50*

d) Organisation des contrôles et des tests d'efficacité

La banque doit savoir et comprendre quels contrôles clés le prestataire externalisé doit réaliser en lien avec la confidentialité des CID. Le respect des exigences internes ainsi que l'efficacité des contrôles doivent être contrôlés et évalués. 51*

II. Glossaire

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. 52*

Grandes quantités de CID : quantité de CID qui, rapportée au nombre total des comptes/à la taille totale du portefeuille de particuliers, est significative. 53*

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, plateformes 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. 54*

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. 55*

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 (hautement) privilégié aux CID (p. ex. administrateurs de bases de données, collaborateurs du management suprême). 56*

Incident grave 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). 57*

Contrôle clé : un contrôle qui, s'il est défini, implémenté et exécuté dans les règles de l'art, réduit considérablement le risque de violation de la confidentialité des CID. 58*

Traitement des données électroniques de clients

<u>Risque inhérent</u> : risque avant toutes mesures d'atténuation ou de contrôle.	59*
<u>Risque résiduel</u> : risques après prise en compte des mesures d'atténuation ou de contrôle.	60*
Techniques réversibles de traitement des données :	61*
<ul style="list-style-type: none">• <u>Données pseudonymisées (pseudonymisation)</u> : 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 eux 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.	62*
<ul style="list-style-type: none">• <u>Données chiffrées</u> : 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.	63*
Techniques irréversibles de traitement des données :	64*
<ul style="list-style-type: none">• <u>Données anonymisées</u> : 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 identifiable. En vertu de la définition, ces données ne sont/contiennent plus des CID et ne sont pas soumises à la LPD³¹.	65*

³¹ Cf. PFPDT, annexe sur les exigences minimales qu'un SGPD doit remplir, 5.

Liste des modifications



La présente circulaire est modifiée comme suit :

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

Modification du 29 août 2013 entrant en vigueur le 1^{er} janvier 2014.

Nouveau Cm 116

Modifications du 29 août 2013 entrant en vigueur le 1^{er} janvier 2015.

Nouveaux Cm 2.1, 117–137

Cm modifiés 1, 29, 50, 53, 71, 79

Cm abrogés 20–22, 28, 30–44, 64

Autres modifications nouveau titre principal avant Cm 3 et nouvelle numérotation des titres
modification du titre avant Cm 50

Modifications du 27 mars 2014 entrant en vigueur le 1^{er} janvier 2015.

Cm modifiés 1, 9, 10, 11, 12, 13, 14

Modifications du 22 septembre 2016 entrant en vigueur le 1^{er} juillet 2017.

Nouveaux Cm 132.1 à 132.3, 135.1 à 135.12, 136.1 à 136.5

Cm modifiés 2, 53, 117, 118, 119, 121, 122, 128, 130, 132, 133, 134, 135, 136, 137

Cm abrogés 2.1, 123, 124, 125, 126, 127, 131

Autres modifications chap. IV.B : renumérotation des principes

Modifications du 31 octobre 2019 entrant en vigueur le 1^{er} janvier 2020.

Cm modifiés 122, 135, 135.1, 135.6

Les annexes de la circulaire ont été modifiées comme suit :

Modifications du 29 août 2013 entrant en vigueur le 1^{er} janvier 2015.

La numérotation des annexes a été adaptée : l'annexe 2 « Classification des segments d'affaires conformément à l'art. 93 al. 2 OFR » devient désormais l'annexe 1 et l'annexe 3 « Vue d'ensemble pour la classification des types d'événements » devient l'annexe 2.

Nouveau annexe 3

