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 » – révision totale

Circulaire 2013/3 « Activités d'audit » – révision partielle

Rapport sur les résultats de l'audition du 10 mai au 11 juillet 2022

7 décembre 2022

Laupenstrasse 27, 3003 Berne, tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

Éléments essentiels

1. L'initiative en faveur de la révision totale de la circulaire FINMA 2008/21 « Risques opérationnels – banques » a rencontré une large approbation. Les participants de l'audition ont également salué le fait que la nouvelle circulaire consolidait les principes de Bâle, la pratique de surveillance de la FINMA et le contenu de l'autorégulation de l'Association suisse des banquiers dans le domaine du *business continuity management* (BCM).

2. Des associations de banques et de sociétés d'audit, des organisations professionnelles ainsi que des banques et des prestataires individuels ont participé à cette audition publique qui s'est déroulée entre le 10 mai et le 11 juillet 2022. La FINMA a évalué leurs indications et en a tenu compte dans la mesure où elles se révélaient pertinentes.

3. Les participants ont accueilli favorablement l'application du principe de proportionnalité et la conception neutre de la circulaire du point de vue technologique. Certains d'entre eux ont demandé davantage d'allègements alors que d'autres ont réclamé des durcissements ponctuels. La FINMA a adapté les chiffres marginaux concernés lorsque cela se révélait à la fois pertinent et conforme avec les attentes en matière de surveillance.

4. Plusieurs participants ont estimé que le calendrier était trop ambitieux. La FINMA reporte par conséquent la date de l'entrée en vigueur d'une année au 1er janvier 2024.

5. De nombreux participants ont estimé que la définition des données critiques était trop large, au point de couvrir presque l'ensemble des données selon le point de vue adopté. La FINMA a par conséquent adapté cette définition en tenant compte des nombreuses propositions reçues.

6. De nombreuses questions ont été posées sur les délimitations et les dépendances, en particulier entre les différentes catégories de risque, entre le BCM et la résilience opérationnelle ainsi qu'entre les inventaires. La FINMA explique les délimitations et les dépendances dans le rapport d'audition et a adapté les chiffres marginaux correspondants là où cela se révélait pertinent et judicieux.

7. La nouvelle circulaire FINMA « Risques et résilience opérationnels – banques » et la révision partielle de la Circ.-FINMA 13/3 « Activités d'audit » entreront en vigueur le 1er janvier 2024 avec des délais transitoires pour garantir la résilience opérationnelle.

Liste des abréviations

BCM	*Business continuity management*
DRP	*Disaster recovery plan*
ESG	Environnement, société et gouvernance d'entreprise
ITSCM	*IT service continuity management*
LB	Loi du 8 novembre 1934 sur les banques (RS 952.0)
LFINMA	Loi du 22 juin 2007 sur la surveillance des marchés financiers (RS 956.1)
MPDT	*Maximum period of downtime*
OFR	Ordonnance du 1er juin 2012 sur les fonds propres (RS 952.03)
RTO	*Recovery time objective*
TIC	Technologie de l'information et de la communication

1 Introduction

Du 10 mai au 11 juillet 2022, la FINMA a mené une audition relative à son projet de révision totale de la circulaire 2008/21 « Risques opérationnels – banques » et aux adaptations de la circulaire 2013/3 « Activités d'audit ».

2 Prises de position reçues

Les institutions suivantes ont participé à l'audition et ne se sont pas opposés à une publication de leur prise de position[1] (par ordre alphabétique) :

- Amazon Web Services (AWS)
- Association suisse des banquiers (ASB)
- Clientis SA
- Credit Suisse Group SA (Credit Suisse)
- EXPERTsuisse
- Institute of Internal Auditing Switzerland (IIAS)
- NCC Group
- Raiffeisen Suisse
- SIX Group SA (SIX)
- Union des Banques Cantonales Suisses (UBCS)

3 Résultats de l'audition et évaluation par la FINMA

Les prises de position reçues sont résumées, pondérées et analysées par la FINMA dans le présent rapport. Sans autre indication, les renvois aux chiffres marginaux se réfèrent aux versions des circulaires soumises à audition.

Ce rapport a été approuvé par le conseil d'administration de la FINMA (art. 11 al. 4 de l'ordonnance relative à la loi sur la surveillance des marchés financiers). Il est publié simultanément aux réglementations approuvées et aux prises de position résultant de l'audition.

[1] Ne sont pas mentionnés ici les participants à l'audition qui n'ont pas souhaité la publication de leur prise de position par la FINMA.

3.1 Généralités, page de garde, objet et champ d'application (Cm 1 et 2)

Prises de position

EXPERTsuisse relève que les personnes au sens de l'art. 1*b* LB devraient aussi être citées comme destinataires sur la page de garde et être comprises dans le terme générique d'« établissements » au Cm 2.

Clientis SA estime que l'organisation de la circulaire en différents principes est inopportune, car elle réglemente des domaines spécifiques et non des principes. Il faudrait les remplacer par des titres de chapitre explicites.

Appréciation

La FINMA approuve la position d'EXPERTsuisse de nommer également les personnes selon l'art. 1*b* LB. Elle estime également que la remarque de Clientis est pertinente et utilise dorénavant des titres de chapitre à la place des « principes ».

Conclusion

Les personnes selon l'art. 1*b* LB sont mentionnées au Cm 2. Au chapitre IV, les titres des sous-chapitres sont remplacés et le terme de « principe » supprimé.

3.2 Principe de proportionnalité

Prises de position

En plus des allègements concédés aux banques des catégories 4 et 5, l'ASB, l'UBCS et Clientis SA souhaitent également des allègements pour les banques de la catégorie 3. L'ASB souligne que dans la circulaire, les standards de Bâle ont été mis en œuvre pour toutes les banques en Suisse mais qu'ils s'adressent exclusivement aux très grandes banques internationales (en Suisse : les grandes banques). Une mise en œuvre proportionnelle et fondée sur des principes se révèle ainsi d'autant plus importante.

L'ASB constate en particulier que les aspects spécifiques découlant des Cm 68, 84, 85 et 95 peuvent impliquer un effort disproportionné pour certains établissements de la catégorie 3. L'UBCS souhaite concrètement que les Cm 31, 33, 34, 61, 68, 84, 85, 88, 90, 91 et 97 ne s'appliquent pas aux établissements de la catégorie 3. EXPERTsuisse explique pourquoi le Cm 69 (annonce des incidents en lien avec les données critiques) est aussi important pour les établissements selon les art. 47*a* à 47*e* OFR, les personnes selon l'art. 1*b* LB ainsi que les maisons de titres qui ne gèrent pas de

comptes et, par conséquent, que l'obligation d'annoncer devrait être réintroduite pour ces établissements. En outre, Clientis SA recommande de réorganiser les chiffres marginaux, de telle sorte qu'au début de chaque domaine thématique apparaissent d'abord les aspects fondamentaux qui concernent l'ensemble des établissements.

Appréciation

Les standards de Bâle s'adressent aux banques actives sur le plan international ; en Suisse, il ne s'agit pas seulement des grandes banques. La mise en œuvre de normes internationales, telles que les standards de Bâle, fait partie de la stratégie du Conseil fédéral concernant les marchés financiers et est prévue à l'art. 7 al. 2 let. d LFINMA.

Il est fait référence au Cm 17, selon lequel les principes doivent être mis 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. Ce principe de proportionnalité s'applique à tous les chiffres marginaux et en particulier aussi aux établissements de la catégorie 3. Par conséquent, la FINMA renonce à introduire un échelon d'allègements en plus pour les établissements de la catégorie 3.

Le sens du Cm 97 n'a pas été compris et a donc été adapté et complété ; cf. chapitre 3.11.2. Le Cm 84 maintient le statu quo car, par analogie, il fait déjà partie des recommandations de l'ASB en matière de *business continuity management* (BCM) publiées en août 2013. Le Cm 34 est limité aux banques d'importance systémique (catégories 1 et 2) ; cf. chapitre 3.5.4.

Les autres chiffres marginaux mentionnés spécialement sont également considérés comme très pertinents pour les établissements de la catégorie 3 et sont donc conservés. L'annonce des incidents (Cm 69) est réintroduite pour les établissements selon les art. 47*a* à 47*e* OFR, les personnes selon l'art. 1*b* LB ainsi que les maisons de titres qui ne gèrent pas de comptes. L'ordre des chiffres marginaux privilégie une structure de fond pertinente ; pour cette raison, il n'est pas procédé à un échelonnement des chiffres marginaux par catégorie.

Conclusion

Le Cm 34 est exclu pour les établissements de la catégorie 3 et le Cm 97 est adapté. Le Cm 69 est réintroduit pour les établissements selon les art. 47*a* à 47*e* OFR, les personnes selon l'art. 1*b* LB ainsi que les maisons de titres qui ne gèrent pas de comptes.

3.3 Définitions

3.3.1 Définition des risques opérationnels (Cm 3)

Prises de position

L'ASB demande de clarifier si la « perte » citée est purement une perte financière ou si elle implique aussi des conséquences dans d'autres secteurs, telle la réputation par ex. Il n'est pas clair non plus si les risques juridiques et les risques de réputation doivent être traités comme des catégories de risque propres ou comme des types de dommages (conséquences). Dans le premier cas, l'ASB demande de délimiter les risques juridiques des risques de *compliance*. Cette délimitation est aussi importante pour l'UBCS car le rapport explicatif (p. 10 et 11) est perçu comme contradictoire à cet égard. En outre, l'ASB demande une délimitation par rapport aux risques ESG, en particulier les risques climatiques. EXPERTsuisse considère qu'une simple répétition de la définition des risques opérationnels selon l'art. 89 OFR est insuffisante et propose que la définition soit plus détaillée, en intégrant explicitement les risques de *compliance* notamment.

Raiffeisen Suisse demande aussi des précisions concernant la définition et les délimitations ainsi que des clarifications si les cas en lien avec des risques juridiques et des risques de *compliance* avec d'éventuelles conséquences sur la réputation doivent être exclus des risques opérationnels. Elle souhaite en plus une énumération illustrant tous les risques opérationnels (en particulier les risques fiscaux), l'intégration des explications concernant la libre circulation des services transfrontières dans la description des risques de *compliance* ainsi qu'une clarification des risques à surveiller par le contrôle des risques ou par la fonction de *compliance*. Selon la Circ.-FINMA 2017/1 « Gouvernance d'entreprise – banques », cette fonction doit en effet évaluer chaque année les risques de *compliance*.

Appréciation

La FINMA s'appuie fondamentalement sur les standards de Bâle. Dans le projet d'audition, elle a par conséquent repris précisément la définition des risques opérationnels qui y figure. Cette définition s'appuie sur les standards de Bâle pour la détermination des exigences en matière de fonds propres. Du point de vue historique, elle se réfère donc purement aux pertes financières. Difficiles à quantifier, les risques de réputation en lien avec les exigences en matière de fonds propres ont été exclus du point de vue historique. Cette exclusion ne signifie pas toutefois que dans la gestion des risques opérationnels, les événements liés aux risques opérationnels sont à exclure dès qu'ils ont potentiellement des répercussions négatives sur la réputation. La FINMA salue et soutient le fait que la gestion des risques opérationnels ait continué à se développer et que d'autres types de dommages, en plus des incidences financières, soient utilisés pour évaluer les risques

opérationnels, comme les répercussions sur la réputation, la clientèle ou le marché, ou encore les conséquences réglementaires (par ex. mesures de surveillance potentielles, perte de la licence bancaire).

Selon la FINMA, le lien avec la perte financière reste pertinent, car d'autres types de dommages peuvent aussi aboutir à leur tour à des pertes financières, même indirectement. Si par ex. les conséquences d'une cyberattaque ne sont pas directement quantifiables précisément, ils peuvent néanmoins se traduire par une perte de confiance de la part de la clientèle, qui aboutit à un recul du chiffre d'affaires. D'autres conséquences négatives sur la réputation et/ou la perte de clientes et clients peuvent aussi mener à une baisse du chiffre d'affaires.

La FINMA considère qu'il n'est pas pertinent de prédéterminer une catégorisation des risques opérationnels et une délimitation stricte entre les risques juridiques et les risques de *compliance* ou de définir très précisément des types de risque spécifiques (comme les risques fiscaux). Une certaine liberté et flexibilité est accordée aux établissements pour qu'ils puissent définir la catégorisation en fonction de leurs besoins (cf. principe de proportionnalité). Du point de vue de la surveillance, il importe en définitive que tous les risques opérationnels soient saisis selon une catégorisation définie et que la catégorisation choisie soit appliquée de manière systématique et cohérente. Pour la gestion des risques opérationnels, la catégorisation choisie peut s'appuyer sur des classifications de référence publiquement accessibles, mais elle n'y est pas tenue. Les risques ESG, climatiques et de développement durable ne devraient pas être exclus systématiquement des risques opérationnels car il existe une forte corrélation entre les risques physiques ou également les risques faisant partie de projets de transformation et les risques opérationnels. Ici aussi l'établissement est libre de choisir sa catégorisation et les critères correspondants.

Par risque de *compliance*, on entend dans les grandes lignes le risque que les lois, règles et directives ne soient pas respectées. Comme prévu par la Circ.-FINMA 17/1, ce type de risque est surveillé par la fonction de *compliance*, qui procède également à une évaluation annuelle indépendante. Si le risque de *compliance* peut aussi être considéré comme risque opérationnel, il doit être intégré dans la gestion des risques opérationnels ou l'information doit lui être transmise.

Conclusion

La définition des risques opérationnels est adaptée pour clarifier le lien avec les pertes financières et souligner la pertinence de prendre en compte également d'autres types de dommages dans la gestion des risques opérationnels.

3.3.2 Définition des données critiques (Cm 7)

Prises de position

L'ASB, l'UBCS, l'IIAS, Raiffeisen Suisse et un autre participant de l'audition estiment que la définition des données critiques dans le projet d'audition est trop large. Selon l'ASB et l'UBCS, la définition doit être resserrée afin de ne pas inclure presque l'ensemble des données. L'ASB a également des doutes si les données comprennent uniquement les données électroniques ou aussi les données physiques. Selon elle, différentes données mentionnées dans le projet d'audition sont déjà protégées par la loi sur la protection des données (données personnelles), le code pénal (secrets professionnels) ou le secret professionnel du banquier selon l'art. 47 LB. Pour cette raison, la réglementation supplémentaire par la FINMA est considérée comme ni pertinente ni nécessaire.

Chaque établissement devrait décider lui-même, en tenant raisonnablement compte de ses conditions concrètes, quelles séries de données il convient de distinguer en fonction du risque. L'IIAS demande de préciser la définition pour que la révision soit plus au clair sur ce qu'il convient de vérifier. Pour Raiffeisen Suisse, le passage « données qui doivent être conservées à des fins réglementaires », en particulier, est formulé de façon trop générale. Le principe de l'importance devrait s'appliquer aussi à ces données. Un autre commentaire relève que la large définition des données critiques selon le Cm 68 impliquerait le déploiement d'un suivi très large, qui serait disproportionnel et non nécessaire, pour remplir les objectifs de la circulaire. De plus, l'inventaire selon le Cm 45 est critiqué comme étant très large.

Credit Suisse propose que la définition des données critiques se réfère à une « protection appropriée » en lieu et place d'une « protection particulière ». Selon elle, il faudrait également définir les notions de « données personnelles » et « secrets professionnels » conformément à la loi sur la protection des données et au code pénal. EXPERTsuisse propose que la confidentialité, l'intégrité et la disponibilité soient complétées par la traçabilité. Un autre commentaire demande que seules les données pertinentes pour l'exécution des fonctions critiques soient considérées comme « données critiques ».

Appréciation

Il convient de mentionner que l'utilisation de la terminologie « données critiques » n'est pas fondamentalement nouvelle. La notion de « données critiques et/ou sensibles » est déjà utilisée dans la Circ.-FINMA 08/21 aux Cm 135.3, 135.7, 135.8 et 135.12, qui portent sur l'infrastructure technologique et la protection de la disponibilité, de l'intégrité et de la confidentialité des « données critiques et/ou sensibles ». Dans la nouvelle circulaire, le

terme de « données critiques » est en principe équivalent aux « données critiques et/ou sensibles » dans la Circ.-FINMA 08/21. Selon la FINMA, la définition contenue dans le projet d'audition est dès lors interprétée plus largement que prévue par les participants de l'audition. Par conséquent, la FINMA précise la définition des données critiques en mettant l'accent sur le caractère important conformément aux propositions de formulation reçues. Les données critiques sont des données qu'un établissement considère – selon sa propre appréciation – comme importantes. Elles incluent aussi bien des données électroniques que physiques. Il est envisageable qu'un établissement ne considère aucune donnée physique comme critique.

Toutefois, dans le cadre de son activité de surveillance, la FINMA n'acceptera pas qu'un établissement estime qu'aucune de ses données n'est critique. Une telle évaluation sera sans doute considérée comme irréaliste allant de pair avec une gestion des risques insuffisante. De plus, les données déjà couvertes par des lois (comme les données personnelles selon la loi sur la protection des données, les secrets professionnels selon le code pénal ou les secrets professionnels du banquier selon la loi sur les banques) ne peuvent pas être systématiquement exclues. Les lois mentionnées et la nouvelle circulaire poursuivent des objectifs distincts, en particulier parce que cette dernière porte sur la gestion des risques. L'orientation de la nouvelle circulaire sur la gestion des risques en matière de données critiques tient compte de la rapide évolution des conditions du marché, en particulier de l'accélération de la numérisation et des pratiques internationales.

La FINMA estime que la restriction des données critiques aux seules données qui sont nécessaires à l'exécution des fonctions critiques (au sens de la garantie de la résilience opérationnelle) est trop limitative ; cf. chapitre 3.11.1. Toutefois, elle considère que l'intégration concrète de la « traçabilité » comme objectif supplémentaire va trop loin en ce qui concerne ses attentes en matière de surveillance, bien que les établissements soient évidemment libres de l'intégrer en plus.

Conclusion

La définition des données critiques et en particulier l'orientation sur l'importance sont précisées.

3.3.3 Terminologie sur le BCM (Cm 8 à 10, 12, 13), la résilience opérationnelle (Cm 14 à 16) et leur distinction

Prises de position

L'IIAS souhaite une précision du terme « processus critiques » (Cm 8) et propose de définir en plus le terme de *business impact analysis* dans le chapitre II. Un participant de l'audition demande de restreindre la définition des processus critiques car selon lui, la réalisation des objectifs commerciaux

comme base de définition est trop large. En lieu et place, les processus critiques devraient concerner le maintien du fonctionnement.

L'ASB remarque que le terme d'« interruption importante » au Cm 9 n'était pas d'usage courant jusque-là et qu'il pouvait être lu dans le sens que les établissements, en cas d'interruption de ce type, devaient désormais fonctionner en mode opérationnel (échelon urgence) et non dans l'environnement BCM défini habituellement (stratégique, échelon crise) ; cela pourrait aboutir à des conséquences notables sur les tâches, compétences et responsabilités actuelles. Le terme « important » devrait lui aussi être clarifié au moyen d'une gradation pondérée en fonction des risques. En outre, l'ASB ajoute que la délimitation ou la dépendance du RTO (Cm 10) ainsi que de la *maximum period of downtime* (MPDT), non mentionnée dans le projet d'audition, devrait être clarifiée à l'égard de la tolérance aux interruptions (Cm 15).

Selon EXPERTsuisse, les *disaster recovery plans* (Cm 12) devraient aussi tenir compte des parties tierces et des données critiques qui ont été utilisées pour atteindre les objectifs de rétablissement.

En ce qui concerne la définition des situations de crise (Cm 13), l'ASB, l'UBCS et Credit Suisse signalent l'importance de l'annexe B des recommandations de l'ASB en matière de *business continuity management* (BCM) d'août 2013. Selon eux, cette annexe présente la différence entre crises et incidents ; or elle n'a pas été prise en compte dans le projet d'audition. La distinction est particulièrement pertinente pour pouvoir engager des fournisseurs pour la gestion de crise et non simplement la gestion des incidents *(incident management)*. De plus, une situation de crise ne devrait pas dépendre du type de gestion mais du type de menace.

Selon l'ASB, les ressources énumérées dans la définition des fonctions critiques (Cm 14) ne devraient pas être citées sur un plan parallèle aux activités, processus et services, car elles ne font pas partie des fonctions critiques en tant que telles mais ont été nécessaires pour leur réalisation. De plus, la définition de la résilience opérationnelle devrait être plus clairement délimitée par rapport au BCM, à l'*IT service continuity management* (ITSCM) ainsi qu'à l'*IT security* (les deux derniers ne sont pas mentionnés dans le projet d'audition) et les dépendances devraient être indiquées. Le rôle des « scénarios graves mais plausibles » (Cm 83) dans la résilience opérationnelle n'est pas clair. La circulaire devrait tenir mieux compte des commentaires détaillés figurant dans le rapport explicatif (p. 24 s.). De plus, il faudrait coordonner les scénarios graves mais plausibles entre la BNS et la FINMA.

Appréciation

Le Cm 76 contient déjà l'essentiel d'une *business impact analysis*, de sorte qu'une définition explicite supplémentaire serait redondante. La définition de

la notion de « processus critiques » est revue et délimitée ; désormais, le rapport aux fonctions critiques, et non plus les objectifs commerciaux, apparait au premier plan. Par conséquent, on entend par processus critiques les processus qui sont essentiels à la réalisation des fonctions critiques. Ce qui distingue fondamentalement les processus critiques des fonctions critiques est l'attente selon laquelle les fonctions critiques se composent vraisemblablement plutôt de plusieurs processus et, à titre complémentaire, éventuellement aussi d'autres activités ou services (qu'un établissement ne qualifie potentiellement pas de « processus »). Dans les petits établissements de complexité moindre, il peut arriver qu'une fonction critique corresponde exactement à un seul processus critique.

La comparaison entre le RTO et la tolérance aux interruptions figurant dans le rapport explicatif est supprimée dans les commentaires car elle est considérée comme non pertinente au vu des prises de position reçues. La *maximum period of downtime* (MPDT) reste délibérément de côté car elle ne fait pas obligatoirement partie intégrante du BCM dans tous les contextes. Les assujettis sont libres d'utiliser cette terminologie. Pour définir la tolérance aux interruptions, il s'agit de décider à partir de quel point les conséquences négatives découlant de la défaillance d'une fonction critique ne sont plus tolérables.

Selon le Cm 80 du projet d'audition, le DRP donne des indications sur les « dépendances externes ». Il contient les dépendances à l'égard des parties tierces. Le Cm 46 du projet d'audition précise que des processus de sauvegarde et de restauration appropriés doivent être mis en œuvre. Il contient également des exigences en matière de sauvegarde applicables aux données critiques. Pour cette raison, la FINMA estime qu'une mention plus explicite des parties tierces et des données critiques n'est pas nécessaire.

La FINMA reconnait l'importance de distinguer les incidents des crises et adapte la définition des situations de crise aux propositions de l'ASB, de l'UBCS et de Credit Suisse. En outre, elle remplace le terme « interruption importante » par « incident ou interruption majeurs ». La définition des fonctions critiques est adaptée conformément à la proposition de l'ASB.

Les termes ITSCM et *IT security* ne sont pas introduits de manière explicite à dessein. Ce sont en effet des cadres de référence, dont l'utilisation ne doit bien sûr pas être empêchée par la circulaire. Celle-ci n'a pas pour ambition d'être un cadre global qui inclut l'ensemble des meilleures pratiques disponibles. En lieu et place, elle doit refléter le plus simplement possible les attentes minimales de la surveillance. Le principe de proportionnalité autorise une certaine flexibilité selon la taille, la complexité, la structure et le profil de risque de l'établissement. L'ITSCM soutient la réalisation des services informatiques et donc du BCM, qui soutient à son tour la résilience opérationnelle. L'*IT security*, en revanche, soutient la gestion des cyberrisques ou

peut être considérée comme une partie d'elle. Une gestion solide des cyberrisques soutient la résilience opérationnelle de l'établissement. La distinction entre le BCM et la résilience opérationnelle est clarifiée au moyen d'adaptations ou de compléments aux définitions concernées.

Les scénarios graves mais plausibles ne sont pas prédéfinis par la FINMA. Il existe en effet une coordination étroite entre la FINMA et la BNS lorsque des activités de surveillance ont lieu conjointement. Une partie de ces dernières est d'ailleurs aussi consacrée à la garantie de la résilience opérationnelle.

Conclusion

Les définitions des situations de crise et des fonctions critiques sont adaptées conformément aux propositions reçues. La définition des processus critiques est elle aussi délimitée pour que son rapport avec les fonctions critiques apparaisse désormais au premier plan. La distinction entre le BCM et la résilience opérationnelle est clarifiée au moyen d'adaptations et de compléments aux définitions terminologiques concernées. Il est renoncé à une définition complémentaire explicite de *business impact analysis*, à une adaptation de la définition de DRP et aux mentions explicites de la MPDT, de l'ITSCM et de l'*IT security*.

3.4 Organe responsable de la haute direction et direction (Cm 21 à 23, 35, 39, 53, 59, 60, 75, 89)

Prises de position

L'ASB remarque que certaines tâches et compétences qui sont transférées à l'organe responsable de la haute direction et à la direction apparaissent trop détaillées et, par conséquent, non conformes au niveau de responsabilité. En particulier, le choix terminologique « mettre en œuvre », qui revient à plusieurs reprises, devrait être remplacé par « assurer », par ex. Il n'est toujours pas clair si l'organe responsable de la haute direction doit adopter l'ensemble des risques opérationnels ou seulement les « risques principaux ». Clientis SA est d'avis que les chapitres sur la gestion des risques TIC, le BCM et la résilience opérationnelle en matière de gouvernance et de processus sont trop détaillés.

Selon l'IIAS, il manque une précision concernant le rôle de l'organe responsable de la haute direction en matière d'externalisations (importantes et non importantes). La circulaire FINMA 2018/3 « Outsourcing » n'est pas assez explicite à ce sujet et le projet d'audition ne le traite pas non plus. Pour ces raisons, l'IIAS recommande en plus une révision de la Circ.-FINMA 18/3.

Appréciation

En matière de gouvernance, la nouvelle circulaire a pour objectif de préciser les attentes envers l'organe responsable de la haute direction ainsi que la direction en lien avec la gestion des risques opérationnels et désormais aussi de la garantie de la résilience opérationnelle. La nécessité de procéder à ces précisions découle de l'expérience historique de la FINMA ; il existe en effet des cas pour lesquels l'organe responsable de la haute direction et la direction n'assument pas leurs obligations à la hauteur des attentes. De plus, la conscience de leur responsabilité manque dans ce sous-domaine de la gestion des risques à l'échelle de l'établissement.

Pour plus de transparence, la FINMA consolide les attentes envers l'organe responsable de la haute direction et la direction, qui se recoupent en partie mais étaient présentées jusque-là séparément, dans quelques chiffres marginaux au début du chapitre sur la gestion des risques opérationnels. Seules les attentes très spécifiques liées aux domaines concernés sont conservées dans les sous-chapitres correspondants. Les textes y relatifs ont eux aussi été revus pour clarifier davantage les attentes. Conformément à la proposition reçue, le terme « mettre en œuvre » est remplacé par « assurer ».

En ce qui concerne les décisions mentionnées par l'IIAS sur les externalisations, la FINMA part du principe qu'elles font partie des stratégies approuvées par l'organe responsable de la haute direction. Il est attendu qu'au moins la stratégie TIC contienne des décisions sur les externalisations. Elles peuvent également être pertinentes pour les stratégies en matière de cyberrisques, de données critiques et de BCM. La FINMA part également du principe que les risques liés aux externalisations sont identifiés, évalués, limités et surveillés comme partie intégrante de la gestion des risques opérationnels. Par conséquent, ils devraient être pris en compte dans la tolérance aux risques que l'organe responsable de la haute direction doit approuver. Prendre une décision sur la tolérance aux risques peut impliquer que l'organe responsable de la haute direction ne soit pas disposé à assumer les risques associés à une externalisation et, partant, y renonce pour des raisons stratégiques.

Conclusion

Les chiffres marginaux relatifs aux attentes envers l'organe responsable de la haute direction et la direction font l'objet d'une révision ainsi que d'une consolidation là où cela se révèle pertinent. Une révision de la Circ.-FINMA 18/3 n'est pas prévue pour l'instant.

3.5 Gestion des risques opérationnels

3.5.1 Tolérance aux risques pour les risques opérationnels (Cm 22, 31)

Prises de position

L'ASB relève que la surveillance de la tolérance aux risques pour les risques opérationnels dans le domaine des risques inhérents, en particulier des cyberrisques, semble difficile à mettre en œuvre. Elle recommande par conséquent d'examiner d'autres approches qui, par ex., sont fondées sur des stratégies de gestion des risques correspondants. Credit Suisse remarque que les indicateurs de contrôle ne pourraient pas être utilisés aux fins de mesure des risques inhérents. Seuls les indicateurs de risque pourraient remplir cette fonction.

Selon EXPERTsuisse, de nombreux établissements ont des incertitudes concernant la terminologie « tolérance aux risques » et « appétit pour le risque ». Elle recommande par conséquent d'utiliser uniquement le terme d'« appétit pour le risque » et de le définir expressément. Compte tenu des insécurités qu'elle a observées lors de la mise en œuvre, elle recommande en outre d'introduire une note de bas de page explicative sur la tolérance aux risques liée aux risques inhérents.

Appréciation

Le terme de « tolérance aux risques » provient de la Circ.-FINMA 17/1. La nouvelle circulaire présente les aspects à prendre en compte en matière de tolérance aux risques dans le domaine des risques opérationnels. Dans la pratique, les assujettis utilisent souvent une terminologie complémentaire comme l'appétit pour le risque ou la capacité de risque. La FINMA est ouverte à l'utilisation d'une autre terminologie ou à une structure plus détaillée tant que le concept de base est couvert. Par conséquent, elle renonce à renommer le terme de « tolérance aux risques » ou à introduire d'autres termes apparentés.

Dans le domaine des cyberrisques, la FINMA relève que la surveillance du risque inhérent est possible, par ex. par la surveillance de la *threat intelligence* et de la situation des menaces ou d'autres réflexions à ce sujet, là où il existe des risques inhérents accrus (comme les systèmes IT accessibles sur Internet). La FINMA est d'accord avec Credit Suisse quand cette dernière affirme que pour mesurer les risques inhérents, seuls les indicateurs de risque sont pertinents, alors que pour mesurer les risques résiduels, il est possible d'utiliser aussi bien des indicateurs de risque que des indicateurs de contrôle. Sur la base de son expérience historique issue des contrôles sur place, la FINMA approuve en outre l'évaluation d'EXPERTsuisse selon

laquelle il existe souvent des incertitudes lors de la mise en œuvre de la tolérance aux risques en lien avec les risques inhérents et que des précisions sont par conséquent judicieuses.

Conclusion

Le Cm 31 est adapté et une note de bas de page ajoutée.

3.5.2 Autres exigences de la part de la FINMA (Cm 24)

Prises de position

L'ASB et l'UBCS proposent un ajout au Cm 24. Selon elles, ce chiffre marginal doit désormais être complété par la définition d'autres exigences par la FINMA si « la gestion d'une situation de risque significative pour un établissement l'exige ». Actuellement, il est en effet formulé de manière ouverte et générale et octroie à la FINMA une marge de manœuvre trop large. Selon Raiffeisen Suisse, le chiffre marginal doit indiquer que la FINMA s'appuie dans ce cadre sur des exigences légales ou réglementaires existantes.

Appréciation

Le Cm 24 du projet d'audition existe déjà sur le fond dans l'actuelle Circ.-FINMA 08/21 (Cm 138) dans le contexte des risques opérationnels de grande portée. Selon ce chiffre marginal, la FINMA définit si nécessaire, dans le cadre de sa surveillance courante, d'autres exigences en matière de gestion des risques opérationnels pour des thèmes spécifiques. Elles sont adoptées avec retenue et en application du principe de proportionnalité. Par expérience, ce Cm est appliqué extrêmement rarement et uniquement en raison de risques opérationnels très élevés, dont la gestion est considérée comme insuffisante. Du point de vue de la FINMA, la formulation proposée par l'ASB et l'UBCS soulève potentiellement des questions supplémentaires concernant la définition d'une « situation de risque significative ». L'audition a donné lieu à de nombreux souhaits de précisions concernant la définition de termes comme « teneur en risque » ou « activités ». La formulation proposée par Raiffeisen Suisse est évidente, de sorte que selon la FINMA, elle n'apporte aucune plus-value. Par conséquent, la FINMA renonce aux compléments proposés.

Conclusion

Le Cm 24 est conservé tel quel.

3.5.3 Examen indépendant des contrôles clés (Cm 28)

Prises de position

L'ASB, l'UBCS, Credit Suisse, EXPERTsuisse et l'IIAS ont indiqué que la définition du terme d'indépendance en lien avec l'examen « indépendant » de l'efficacité des contrôles clés devait être étayée. Ils s'interrogent en particulier si i) l'examen indépendant pourrait être effectué par un membre de l'équipe ou le supérieur hiérarchique, ou une division séparée au sein de la première ligne de défense et si ii) l'indépendance se réfère à la deuxième et troisième ligne de défense ou seulement à l'une des deux.

En outre, EXPERTsuisse ajoute que les résultats de l'examen indépendant devraient être documentés de façon compréhensible et que les éventuelles faiblesses identifiées devraient être traitées rapidement.

Appréciation

Il est à noter que les unités porteuses de risques (c.-à-d. la première ligne de défense, dont en particulier les unités d'affaires génératrices de revenus) sont responsables de garantir l'efficacité des contrôles clés relatifs aux risques opérationnels qu'elles ont encourus et qu'elles sont tenues de prendre des mesures appropriées (par ex. examen structuré de l'efficacité des contrôles clés).

Au sens des « Revisions to the Principles for the Sound Management of Operational Risks »[2] du Comité de Bâle sur le contrôle bancaire, sur lesquelles s'appuie la nouvelle circulaire, la FINMA précise que l'examen « indépendant » mentionné au Cm 28 doit être effectué par des instances de contrôle indépendantes conformément à la Circ.-FINMA 17/1. Cela signifie que l'examen indépendant est réalisé par le contrôle des risques et/ou la fonction de *compliance*, ou encore – s'il en existe une – par l'unité qui regroupe le contrôle des risques et la fonction de *compliance*.

Compte tenu de l'expérience historique issue des contrôles sur place, la FINMA approuve la position d'EXPERTsuisse selon laquelle les examens indépendants doivent être documentés de façon compréhensible. Sans documentation appropriée, les évaluations concernant l'efficacité des contrôles clés ne sont ni justifiables ni compréhensibles, ce qui peut se traduire par une remise en question de l'efficacité du système de contrôle interne.

[2] https://www.bis.org/bcbs/publ/d515.pdf; cf. en particulier Cm 10 « *A functionally independent CORF is typically the second line of defence. The responsibilities of an effective second line of defence should include: a) developing an independent view regarding business units' […] (ii) design and effectiveness of key controls, […]* », où le CORF en question est une « Compliance and Operational Risk Function » (cf. note de bas de page 6 « *In addition to an independent Operational Risk Management function, the second line of defense also typically includes a Compliance function.* »).

Toutefois, à l'encontre de la recommandation d'EXPERTsuisse, la FINMA renonce à préciser que les éventuelles faiblesses identifiées doivent être traitées rapidement. Des faiblesses de ce type doivent être reconnues et communiquées de façon transparente (Cm 33), mais l'une des réponses possibles consiste aussi à accepter expressément le risque qui en découle.

Conclusion

La première phrase du Cm 28 dans le projet d'audition est adaptée.

3.5.4 Autres prises de position concernant la gestion des risques opérationnels

Prises de position

EXPERTsuisse propose que les risques associés au BCM et à la résilience opérationnelle soient également pris en compte comme partie intégrante de la gestion des risques opérationnels (Cm 21). L'ASB s'interroge si la catégorisation des risques opérationnels selon le Cm 25 reste unique et si les rapports doivent être réalisés selon cette catégorisation.

D'après EXPERTsuisse, il est nécessaire d'évaluer les risques de façon « formelle et compréhensible » (Cm 26). Les cyberattaques devaient être mentionnées comme exemples de facteurs externes possibles (note de bas de page 5). La différence entre résultats d'audit et évaluations des contrôles n'est pas claire pour Raiffeisen Suisse (Cm 27) car selon elle, l'objectif d'un audit consiste à évaluer l'adéquation et l'efficacité d'un contrôle. Elle recommande de fusionner les deux termes.

Pour l'UBCS, le terme « activités » au Cm 29 n'est pas compréhensible et devrait être défini de manière exhaustive. EXPERTsuisse relève à propos de ce chiffre marginal que les évaluations des risques et des contrôles sont effectuées avant d'apporter des modifications importantes et que de nouvelles mesures de contrôle et d'atténuation devraient être introduites consécutivement. Pour l'UBCS, le terme « teneur en risque » du Cm 30 n'est pas clairement défini et devrait être remplacé par « risque ».

L'UBCS indique que le compte rendu du contrôle des risques mentionné au Cm 32 n'est pas approprié pour fournir des résultats d'audit importants et aboutirait à un doublon avec les prescriptions prévues dans la Circ.-FINMA 17/1 pour l'appréciation des rapports d'audit par l'organe responsable de la haute direction. Raiffeisen Suisse recommande de supprimer l'obligation de rendre compte sur le plan des domaines commerciaux ou organisationnels (Cm 34), car les responsabilités seraient déterminées sur le plan de la direction.

Appréciation

La FINMA reprend les propositions d'EXPERTsuisse (Cm 21, 26, 29), qu'elle considère comme pertinentes, tout comme les propositions de l'UBCS concernant les Cm 30 et 32.

Les risques opérationnels devraient pouvoir être attribués clairement aux classes de catégorisation selon le Cm 25 à l'aide d'une procédure ou de critères définis par l'établissement. La catégorisation choisie devrait être appliquée systématiquement dans toutes les composantes de la gestion des risques opérationnels, c.-à-d. aussi dans le rapport sur les risques opérationnels.

Les évaluations des risques et des contrôles (Cm 27) se distinguent clairement des audits. Les évaluations des risques et des contrôles sont effectuées par les unités opérationnelles et organisationnelles porteuses des risques (y compris les unités d'affaires génératrices de revenus), en ce qui concerne les risques opérationnels qui sont pertinents pour l'unité concernée. Les audits sont réalisés par la révision interne, la société d'audit externe ou d'autres parties indépendantes et couvrent un ou plusieurs domaines thématiques spécifiques à définir à l'avance.

Compte tenu de la diversité des assujettis et de leurs modèles d'affaires concernés par la nouvelle circulaire, la FINMA renonce à définir plus précisément le terme « activités » (Cm 29). Une définition plus précise serait forcément trop restreinte et ne pourrait pas rendre compte de l'hétérogénéité des assujettis.

Le rapport sur le plan des domaines commerciaux ou organisationnels (Cm 34) est surtout pertinent pour les établissements de complexité élevée et avec une structure de groupe. La FINMA restreint par conséquent ce chiffre marginal aux banques d'importance systémique, bien que le principe de proportionnalité s'applique aussi à ce chiffre marginal, comme à tous les chiffres marginaux de la circulaire.

Conclusion

Les Cm 21, 26, 29, 30 et 32 sont adaptés conformément aux propositions de formulation reçues. Le Cm 25 sur la catégorisation reste identique, mais le Cm 32 sur le rapport est complété afin de clarifier l'utilisation de la catégorisation dans les rapports. Le Cm 34 est limité aux banques d'importance systémique en fonction de leur complexité et de leur structure. Le Cm 27 est conservé tel quel.

3.6 Gestion des risques TIC

Prises de position

EXPERTsuisse recommande un complément pour le Cm 35, selon lequel la direction doit garantir des ressources suffisantes pour atteindre la stratégie TIC. Raiffeisen Suisse demande, en lien avec la gestion des risques TIC au Cm 36 (mais aussi en se référant à la gestion des cyberrisques), s'il y a lieu de requérir des exigences supplémentaires concernant la surveillance et en particulier le compte rendu lorsque l'ensemble des processus TIC sont externalisés.

Pour l'ASB et l'UBCS, l'attente à l'égard de la prise en compte des nouvelles évolutions technologiques au Cm 37 n'est pas claire. EXPERTsuisse propose pour ce chiffre marginal de mentionner des standards internationaux concrets reconnus comme COSO ou COBIT, alors que Raiffeisen Suisse recommande de parler de *good practices* (bonnes pratiques) au lieu de *best practices* (meilleures pratiques), car d'une part ce sont habituellement de bonnes normes sectorielles, et d'autre part tous les établissements n'ont pas à rivaliser avec les meilleurs à l'aide de *best practices*.

L'ASB et l'UBCS se demandent si la formulation du Cm 43 en lien avec la séparation des environnements de développement, de test et de production est trop standard et pas assez orientée sur les risques. EXPERTsuisse recommande de garantir uniquement la séparation avec la production pour tenir compte des méthodes de développement comme *DevOps*. Elle propose également des adaptations de plusieurs autres chiffres marginaux.

L'ASB et l'UBCS remarquent que le terme « besoin de protection » du Cm 47 est nouveau et pas clair concernant sa délimitation par rapport à la tolérance aux risques. La notion de « mesures de protection » au Cm 55 est elle aussi nouvelle.

Pour gérer efficacement les risques opérationnels, y compris les risques TIC, AWS recommande aux établissements d'élaborer un descriptif holistique à l'échelon de l'établissement de leurs activités commerciales et de leurs priorités respectives, ainsi que le personnel, les processus et les technologies nécessaires à cet effet.

Appréciation

La FINMA estime que la demande en ressources suffisantes est déjà assez couverte par le Cm 41 du projet d'audition. Le Cm 36 pose le cadre pour la gestion des risques TIC et traite aussi bien les risques TIC et les cyberrisques que les risques technologiques qui sont liés aux externalisations *(outsourcing)*. À cet égard, l'établissement doit rendre compte régulièrement à la direction de l'évolution des risques, des mesures, des contrôles et des

incidents TIC. La fréquence minimale imposée par la FINMA est d'une fois par année. L'établissement est libre d'adopter une fréquence plus élevée (par ex. trimestrielle).

Le Cm 37 vise à ce que les risques pouvant découler des nouvelles évolutions technologiques soient pris en compte dans l'analyse des risques et dans le SCI de l'établissement. La FINMA renonce à nommer explicitement des standards internationaux reconnus et des *best* ou *good practices* dans la circulaire. COBIT, ITIL, COSO et divers standards ISO, en particulier, sont largement connus et reconnus. Le terme de *practices* (pratiques), admis sur le plan international, est repris.

L'idée du Cm 43 (séparations des environnements) est de souligner la nécessité de conserver une séparation claire entre les environnements TIC pour le développement, le test et la production TIC, indépendamment de la diffusion de méthodes de développement flexibles (modèles DevOps et CI/CD – *continuous implementation – continuous deployment*). Cela comprend dans la mesure du possible une attribution claire de tâches, de fonctions et de responsabilités ainsi qu'une réglementation des autorisations d'accès afférentes. Il s'agit de garantir que les développeurs et les testeurs de codes ou de nouvelles parties ou de parties adaptées de logiciels ne puissent pas les valider eux-mêmes dans l'environnement de production. C'est un contrôle préventif fondamental à la protection de l'entreprise. Le chiffre marginal est adapté en conséquence. Les autres propositions d'EXPERTsuisse sont aussi reprises dans la mesure où elles améliorent, du point de vue de la FINMA, la clarté des chiffres marginaux concernés.

Au Cm 47, le terme « besoin de protection » est supprimé car sa mention n'est pas absolument nécessaire. Dans ce chiffre marginal, il en va en effet des aspects « confidentialité, intégrité et disponibilité ». Les « mesures de protection » au Cm 55 sont conservées et, selon la FINMA, ne nécessitent pas de définition plus étendue.

Conclusion

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les TIC sont désormais synthétisées dans le chapitre consacré à la gestion globale des risques opérationnels. Cela concerne les Cm 35, 36 et 38 à 40 du projet d'audition. Les Cm 37, 42, 43 et 45 à 48 sont adaptés sur la base des retours reçus, dans la mesure où les commentaires sont fondés et pertinents. Le Cm 41 est complété et précisé en conséquence (« séparation des environnements »).

3.7 Gestion des cyberrisques

Prises de position

Clientis SA souhaite un regroupement des chapitres « Gestion des risques TIC » et « Gestion des cyberrisques », car ces deux thèmes présentent de nombreux recoupements.

Pour les trois premiers chiffres marginaux dans la gestion des cyberrisques, l'IIAS souhaite une réglementation plus claire des rôles et des compétences pour l'organe responsable de la haute direction en ce qui concerne la gestion des cyberrisques ainsi qu'une harmonisation avec d'autres chapitres dans la circulaire. Pour le Cm 54, SIX demande un compte rendu au moins trimestriel et non pas annuel à l'intention de la direction.

En ce qui concerne la note de bas de page 8 du Cm 55, l'ASB et l'UBCS réclament que la définition d'une cyberattaque soit limitée à des attaques de l'extérieur vers l'intérieur, par ex. par un franchissement du périmètre. EXPERTsuisse souhaite une déclaration plus explicite si des attaques de la part du personnel interne relèvent également de la définition d'une cyberattaque.

Pour le Cm 55 let. a, EXPERTsuisse propose de parler de risques au lieu de menaces potentielles.

Au Cm 55 let. b, EXPERTsuisse suggère de ne pas limiter l'implémentation de mesures de protection appropriées aux processus critiques mais de mentionner également les systèmes et les données. SIX propose d'ajouter l'engagement / la non-répudiation aux objectifs de protection que sont la confidentialité, l'intégrité et la disponibilité.

Dans l'énumération au Cm 55 let. c concernant la surveillance globale des TIC, l'UBCS voit une violation du principe de proportionnalité et de l'approche par le risque. SIX remarque en outre que dans le même chiffre marginal, l'ordre logique entre détection et enregistrement est inversé.

L'UBCS souhaite que l'obligation d'annoncer les cyberattaques selon la LFINMA, précisée au Cm 56, soit centralisée pour l'ensemble des services administratifs. Un autre commentaire reçu propose ici de supprimer la référence explicite à l'article de la LFINMA sur l'obligation d'annoncer.

L'ASB, Raiffeisen Suisse, EXPERTsuisse ainsi qu'un autre participant demandent une précision sur les cyberexercices fondés sur des scénarios au Cm 58. La formulation peut laisser entendre que ces exercices devraient être effectués dans la même ampleur que les analyses de vulnérabilité et les tests d'intrusion. De même pour le Cm 58, l'ASB demande de délimiter clairement la portée du nouveau volume minimal d'analyses de vulnérabilité et

de tests d'intrusion précisé par la FINMA s'agissant des systèmes IT accessibles sur Internet.

AWS souligne que dans ses prestations, les responsabilités sont partagées avec la clientèle *(shared responsibility model).* Les clients sont ainsi responsables de la sécurité au sein du *cloud* AWS, c.-à-d. de la sécurité des contenus, applications, systèmes et réseaux qu'il contient. En revanche, AWS est responsable de la sécurité du *cloud* même, c.-à-d. que la société protège l'infrastructure sous-jacente et garantit la performance des services.

Appréciation

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les cyberrisques sont désormais synthétisées dans le chapitre consacré à la gestion globale des risques opérationnels.

La FINMA ne répond pas au souhait de changement de l'ASB et de l'UBCS d'exclure explicitement les menaces émanant de l'intérieur. Les attaques dirigées contre les TIC et les données critiques par l'exploitation de faiblesses ou en contournant des mesures protectrices peuvent aussi être lancées au sein du périmètre. De telles attaques doivent aussi pouvoir être détectées par des moyens appropriés et des contrôles techniques. La note de bas de page a été précisée sur la base du commentaire reçu.

Au Cm 55 let. a, il est mentionné que les établissements analysent d'abord la situation générale des menaces (par ex. les cyberattaques dont ils ont connaissance qui ont touché d'autres entreprises et les outils utilisés ou les faiblesses exploitées dans ce cadre) puis en déduisent les menaces potentielles pour eux-mêmes *(threat intelligence)*. Ce n'est qu'ensuite que les risques spécifiques à un établissement peuvent être identifiés si par ex. un actif vulnérable à cet égard figure dans l'inventaire.

Le Cm 55 let. b est légèrement adapté conformément au commentaire d'EXPERTsuisse. La FINMA estime non pertinente la proposition de SIX d'ajouter la non-répudiation aux trois objectifs de protection visés par les cyberattaques, à savoir la confidentialité, l'intégrité et la disponibilité des données critiques et des systèmes IT. Par des attaques visant la non-répudiation, il n'est plus possible de garantir que l'auteur élabore des informations ou qu'il les a envoyées. La FINMA reconnaît que la non-répudiation est très importante dans le domaine de la sécurité de l'information. Elle est toutefois déjà couverte dans le contexte des cyberrisques ou des attaques par le point concernant l'intégrité.

Le commentaire de l'UBCS concernant l'ampleur de la surveillance à exercer sur les systèmes au Cm 55 let. c est justifié. « Complet » est remplacé

par « constant » avec un renvoi aux composantes TIC répertoriées. Le *feedback* de SIX concernant l'ordre de la procédure de détection est également repris.

L'obligation d'annoncer décrite au Cm 56 a été reprise par la communication FINMA sur la surveillance 05/2020. Elle en précise l'importance et le caractère urgent pour le contexte cyber conformément aux exigences prévues à l'art. 29 al. 2 LFINMA. Depuis la publication de la communication sur la surveillance, d'autres autorités ont aussi annoncé qu'elles planifiaient l'introduction de l'obligation d'annoncer pour les infrastructures critiques. Le projet de loi correspondant est en cours d'élaboration. Dès que le texte réglementaire sur l'obligation d'annoncer sera finalisé, la FINMA examinera si et comment, en tenant compte du secret de fonction selon la LFINMA, un système de notification centralisé commun aux autorités est réalisable en matière de cyberattaques. Compte tenu du commentaire d'un autre participant, le renvoi à l'article et au paragraphe correspondant dans la LFINMA est supprimé.

Le Cm 58 porte sur l'activité qui suit le Cm 55 let. a. Dès que les établissements ont défini leurs propres menaces potentielles, ils doivent analyser les conséquences qu'elles ont sur eux-mêmes. Le paragraphe sur les cyberexercices fondés sur des scénarios a été déplacé dans un chiffre marginal à part par suite des commentaires reçus, afin de conserver le principe de se baser sur les risques. Les analyses de vulnérabilité et les tests d'intrusion devront toujours être effectués régulièrement sur les applications, systèmes ou interfaces minimaux spécifiés. Le rapport explicatif contient des commentaires détaillés sur l'étendue minimale des analyses de vulnérabilité et des tests d'intrusion à réaliser pour les services tiers utilisés (par ex. Twitter).

Conclusion

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les cyberrisques sont désormais synthétisées dans le chapitre consacré à la gestion globale des risques opérationnels. Cela concerne les Cm 48, 49 et 52 du projet d'audition. La note de bas de page 8, qui porte sur la définition d'une cyberattaque, a été précisée. L'étendue de la surveillance des TIC est adaptée au Cm 55 let. c. Au Cm 51, le renvoi à la LFINMA est supprimé. En outre, les exigences à l'égard des exercices de type cyber fondés sur des scénarios sont retirées du Cm 53 et déplacées dans un chiffre marginal séparé. L'étendue minimale pour les analyses de vulnérabilité et les tests d'intrusion est précisée.

3.8 Gestion des risques des données critiques

Prises de position

Selon Clientis SA, la gestion des risques des données critiques doit s'appuyer systématiquement sur la nouvelle législation en matière de protection des données et s'y référer autant que possible. EXPERTsuisse demande de clarifier si la stratégie en matière de données mentionnée au Cm 59 doit être édictée par l'organe responsable de la haute direction, tandis que l'IIAS signale que le rôle de l'organe responsable de la haute direction en matière de gestion des risques des données critiques doit aussi être cité.

L'ASB remarque que la fonction de contrôle indépendante découlant du Cm 60 ne doit pas être seule responsable pour créer et maintenir les conditions cadres mentionnées. Par ailleurs, l'ASB et un autre participant de l'audition demandent s'il s'agit d'une des deux instances de contrôle indépendantes selon la Circ.-FINMA 17/1 (c.-à-d. le contrôle des risques ou la fonction de *compliance*). L'ASB et l'UBCS s'interrogent sur la signification du terme « degré de criticité » au Cm 61 et si on entend par là que les données critiques doivent encore être réparties en sous-catégories.

Selon l'ASB, la disponibilité et l'intégrité des données (par ex. état du compte, montant du crédit) peut dépendre du fait que ces données se trouvent dans un domaine critique de la banque (par ex. système bancaire central) et devraient donc être classées comme critiques seulement temporairement durant leur cycle de vie. Pour cette raison, la gestion de ces données tout au long de leur cycle de vie mentionnée au Cm 62 ne ferait aucun sens. Comme ce qui est entendu par une stratégie complète en matière de données n'est pas clair, le mot « complète » devrait être supprimé.

L'ASB et l'UBCS invitent à définir de manière exhaustive le terme « données authentiques » au Cm 64 ou, à titre de variante, de parler de « données dans les environnements de test ». Credit Suisse propose de parler ici d'une « protection appropriée » au lieu d'une simple « protection », alors qu'EXPERTsuisse suggère de souligner plus nettement que le Cm 64 s'applique aussi aux situations normales. L'ASB regrette que le Cm 66 prescrive un *role based access control*, qui n'est pas toujours le modèle optimal pour la gestion des accès. En lieu et place, elle recommande les principes du *need-to-know* et du *least privilege*.

L'ASB demande la suppression du Cm 67 car la prescription en matière de protection des données critiques qui sont enregistrées à l'étranger découle déjà des Cm 59 et 63 du projet d'audition et qu'il devrait être possible d'introduire une référence à la Circ.-FINMA 18/3. Credit Suisse recommande que ce chiffre marginal mentionne une protection « appropriée » au lieu de « particulière » et que le terme « risques accrus » soit défini plus précisément.

SIX demande de clarifier ce qui est entendu par « protection particulière », cela également au Cm 65.

Au Cm 68, l'ASB n'est pas totalement au clair sur les personnes concernées par la liste mentionnée et comment l'élément « utilisatrices et utilisateurs qui disposent d'un accès fonctionnel à une grande quantité de données critiques » peut être interprété comme élément possible pour considérer une personne comme bénéficiant de privilèges accrus. EXPERTsuisse signale que la terminologie « traitement des données » mentionnée au Cm 70 a déjà été définie à l'art. 3 let. e de la loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1). Du point de vue d'EXPERTsuisse, une exclusion de ce chiffre marginal pour les établissements selon l'art. 47*a* à 47*e* OFR, les personnes selon l'art. 1*b* LB ainsi que les maisons de titres ne tenant pas de comptes est contraire à l'exigence de surveillance des prestataires selon le Cm 24 Circ.-FINMA 18/3, car les accès de prestataires externes à des données critiques proviennent souvent des externalisations de fonctions importantes.

Appréciation

La FINMA n'est pas compétente pour déterminer la portée et l'application du droit de la protection des données. La surveillance dans le domaine du droit de la protection des données incombe au préposé à la protection des données. Par conséquent, la nouvelle circulaire ne contient pas de précisions concernant la législation en matière de protection des données. Cette dernière doit être respectée indépendamment de la circulaire, tout comme les autres lois. La circulaire traite de la gestion des risques qui découlent du traitement des données, avec une priorité d'une part sur les « données critiques » à des fins de délimitation et d'autre part sur leur importance. Pour cette raison, la circulaire n'est pas adaptée à la législation en matière de protection des données et ne contient à cet effet pas de renvoi à cette dernière. Le rôle de l'organe responsable de la haute direction est désormais traité dans le chapitre relatif à la gestion globale des risques opérationnels, cela en particulier aussi en lien avec la stratégie en matière de données et la gestion des risques des données critiques.

Le positionnement de l'unité indépendante en qualité de fonction de contrôle découlant du Cm 60 revient à l'établissement, comme c'était déjà le cas à l'annexe 3 de la Circ.-FINMA 08/21 en lien avec les données électroniques des clients. La formulation du Cm 60 a également été reprise de cette annexe, mais elle sera modifiée dans la nouvelle circulaire. L'objectif du degré de criticité mentionné au Cm 61 est de classer les données du point de vue de leur criticité par rapport aux trois aspects cités : la « confidentialité », l'« intégrité », y compris la non-répudiation, et/ou la « disponibilité ». Ici, une classification plus fine de la criticité est possible, voire pertinente en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement, mais

elle n'est pas impérative pour chaque établissement (cf. principe de proportionnalité). Le lien avec le « degré de confidentialité » est supprimé car il est inclus dans la criticité ou le degré de criticité.

Du point de vue de la FINMA, les données qui sont considérées comme « critiques » sont critiques durant tout leur cycle de vie et doivent être protégées en conséquence. Par exemple, les données de compte critiques restent critiques tout au long de leur cycle de vie, de leur création jusqu'à leur suppression. La FINMA accorde une grande importance au fait que les établissements définissent leurs données critiques en tant que telles et les surveillent en conséquence sur l'ensemble du cycle de vie (durée de vie).

Les « données authentiques » du Cm 64 sont remplacées par « données » conformément à la proposition de l'ASB et de l'UBCS. Les propositions de Credit Suisse et d'EXPERTsuisse sont également reprises dans ce chiffre marginal. Le Cm 66 est adapté pour ne pas être limité à un *role based access control*.

Au Cm 67, le lien avec l'étranger est conservé car il ne découle pas assez clairement des autres chiffres marginaux et reste pertinent même dans les cas qui ne concernent pas une externalisation. Selon la FINMA, un renvoi à la Circ.-FINMA 18/3 est donc insuffisant. Dans les Cm 7, 65 et 67, le terme « particulier » a été délibérément préféré à « approprié » pour souligner la protection spéciale de ces données. Cela exprime ainsi avec emphase qu'il faut garantir une protection plus élevée qu'avec d'autres données non critiques. Les établissements doivent engager leurs ressources de manière pertinente et veiller à ce que leurs données critiques soient assurées par des mesures particulières comme des réglementations d'accès privilégié, le respect du principe *need-to-know* ainsi que le cryptage des données. Les établissements doivent mettre en œuvre un modèle d'accès approprié qui permet le respect des principes *need-to-know* et *least privilege*. Les droits d'accès déposés doivent être régulièrement contrôlés.

Les propositions d'EXPERTsuisse en lien avec le traitement des données critiques au Cm 70 sont reprises.

Conclusion

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les données critiques sont désormais synthétisées dans le chapitre consacré à la gestion globale des risques opérationnels. Cela concerne le Cm 59 du projet d'audition. Le Cm 60 est adapté pour clarifier le fait que le positionnement de l'unité mentionnée revient à l'établissement. Les Cm 61 et 64 à 70 sont adaptés conformément aux propositions de formulation reçues.

3.9 Gestion des risques liés aux activités de service transfrontières

Prises de position

L'IIAS remarque que le rôle de l'organe responsable de la haute direction n'est pas précisé dans ces prescriptions. Selon lui, il serait judicieux de mentionner certains aspects supplémentaires comme l'analyse des risques, la définition du périmètre de la zone d'activité géographique et le compte rendu de la direction à l'organe responsable de la haute direction. Credit Suisse recommande de parler d'une analyse « appropriée » au lieu d'une analyse « approfondie » au Cm 72.

L'ASB constate qu'au terme des délais transitoires, tant les banques que les gestionnaires de fortune indépendants (GFI) opéreront en tant qu'établissements financiers licenciés et assujettis à part entière. Les banques dépositaires n'auraient connaissance que d'une partie des activités des GFI. Dans certains domaines, elles n'auraient par conséquent aucune possibilité de vérifier l'exhaustivité et la plausibilité des informations fournies. Dès lors, elles auraient besoin d'informations concernant les audits auxquels procéderont les nouveaux organismes de surveillance en ce qui concerne le respect des obligations découlant de la loi sur les services financiers du 15 juin 2018 (RS 950.1) ainsi que de la loi sur les établissements financiers du 15 juin 2018 (RS 954.1). Ces données seraient intégrées dans la future organisation de gestion des risques découlant des relations d'affaires avec des GFI. L'ASB s'attend à ce que les responsabilités des banques dépositaires soient délimitées par rapport à celles des GFI et de leurs propres organismes de surveillance ainsi que de la FINMA. Un échange avec la FINMA est en cours à ce sujet.

Appréciation

La FINMA s'attend à ce que les risques découlant des activités de service transfrontières fassent partie des décisions de l'organe responsable de la haute direction concernant la tolérance aux risques. Ils devraient aussi faire partie des évaluations des risques et des contrôles, dont les résultats sont présentés à l'organe responsable de la haute direction. En matière de tolérance aux risques, l'organe responsable de la haute direction pourrait par ex. décider de ne plus être disposé à assumer les risques qui découlent des activités d'un établissement dans un pays précis, et par conséquent d'adapter sa stratégie en modifiant la présence géographique de l'établissement. La FINMA considère par conséquent qu'il n'est pas nécessaire de nommer explicitement le rôle de l'organe responsable de la haute direction dans ce sous-chapitre consacré à la gestion des risques liés aux activités de service transfrontières.

Il est en revanche apparu que la phrase « En tant qu'autorité de surveillance, la FINMA s'attend en particulier à ce que les banques respectent le droit étranger de la surveillance. » n'a aucune autre signification spécifique que des explications d'ordre général sur les exigences prudentielles en matière de gestion des risques juridiques découlant des activités de service transfrontières. Elle découle déjà des exigences générales en matière de gestion des risques juridiques et peut donc être supprimée. Le critère d'appréciation d'une violation du droit de la surveillance suisse du fait du non-respect du droit étranger se fonde donc toujours sur les exigences générales telles qu'elles ressortent du chapitre F et des exigences relatives à la garantie d'une activité irréprochable. La suppression de la phrase mentionnée n'entraîne donc aucune modification matérielle ou réglementaire.

En ce qui concerne la prise de position de l'ASB, un dialogue est en cours avec la FINMA comme mentionné plus haut par l'ASB. Sur la base de l'audition, la FINMA ne voit pas la nécessité d'adapter les chiffres marginaux relatifs aux activités de service transfrontières.

Conclusion

La phrase « En tant qu'autorité de surveillance, la FINMA s'attend en particulier à ce que les banques respectent le droit étranger de la surveillance. » est supprimée. Les autres chiffres marginaux concernant la gestion des risques liés aux activités de service transfrontières restent inchangés.

3.10 *Business continuity management*

Prises de position

Selon l'ASB, il faut mentionner le terme « exercice » en plus du terme « test », car certains contrôles peuvent être effectués uniquement sous la forme d'exercices *table-top*, par ex.

De plus, l'ASB et l'UBCS remarquent que les tests annuels (ou des exercices) représentent une charge trop élevée (Cm 84). En lieu et place, il faudrait les réaliser régulièrement en fonction des risques et coordonner par conséquent leur fréquence avec le compte rendu régulier selon le Cm 87. L'IIAS recommande en revanche de définir une fréquence minimale fixe aussi pour l'approbation de la stratégie BCM (Cm 75) et le compte rendu (Cm 87).

En outre, l'ASB remarque que selon sa compréhension, les « scénarios graves mais plausibles » présentent un caractère distinctif entre le BCM et la résilience opérationnelle. Par conséquent, les tests dans le BCM ne devraient pas se référer à de tels scénarios (Cm 86).

L’ASB et un autre participant interprètent le Cm 80 dans le sens qu’il ne peut exister qu’un seul DRP par établissement. Or il devrait aussi être possible pour les grands établissements de définir plusieurs DRP. EXPERTsuisse recommande de parler de « processus critiques » externalisés au Cm 80 au lieu de « parties de l’infrastructure technologique » externalisées. Elle recommande en outre de préciser le Cm 79 dans le sens que la *business impact analyse* (BIA) et le *business continuity plan* (BCP) doivent aussi être clairement actualisés ad hoc à la suite de changements importants.

Selon Clientis SA, le chapitre doit être rigoureusement harmonisé avec la Circ.-FINMA 18/3. Dans toute la mesure du possible, il faudrait introduire un renvoi à la Circ.-FINMA 18/3 au lieu d’édicter des règlements complémentaires, en particulier en ce qui concerne le Cm 80. Il faudrait tenir compte du fait que les banques des catégories 3 à 5 ont externalisé la plus grande partie de leur infrastructure et de nombreux processus critiques à des prestataires externes.

Appréciation

Du point de vue de la FINMA, le terme « tests » comprend également des « exercices », en particulier aussi des exercices *table top*, des *desktop reviews* et des *walkthroughs*. C’est ce qui ressort du Cm 83 dans le projet d’audition (« Il est possible de choisir plusieurs manières de procéder au test avec des degrés d’intensité et d’efficacité variables »). Selon le souhait de l’ASB, la FINMA introduit en plus le terme d’« exercices », mais l’intègre toutefois comme auparavant sous les « tests ».

Les recommandations de l’ASB en matière de *business continuity management* (BCM) d’août 2013 contenaient déjà la recommandation de tester au moins une fois par année les mesures les plus importantes et l’organisation de crise. Le Cm 84 du projet d’audition formulé en conséquence correspond ainsi au statu quo. Toutefois, il n’est appliqué qu’aux établissement des catégories 1 à 3, de sorte que les petits établissements disposent de davantage de flexibilité ici. La fréquence d’approbation de la stratégie pour le BCM et le compte rendu est harmonisée avec les autres domaines thématiques (TIC, cyberrisques, risques des données critiques). La définition de la stratégie BCM est aussi supprimée à des fins de concordance.

Comme le BCM représente une composante importante pour soutenir la résilience opérationnelle, la FINMA estime qu’il est logique et pertinent de traiter les scénarios graves mais plausibles déjà dans le cadre du BCM.

Selon la FINMA, il peut bien entendu exister plusieurs DRP en fonction de la taille, de la complexité et de la structure de l’établissement. À des fins de clarification, elle reformule le Cm 80 en précisant que l’établissement définit « au moins un DRP ». Lors de l’utilisation de plusieurs DRP, il est important qu’ils parviennent à une couverture suffisante et cohérente des risques. Par

ex. ils ne doivent donner lieu à aucun conflit entre les processus de rétablissement fixés dans les divers DRP. De plus, aucune composante importante ne doit être perdue car chaque unité organisationnelle ne veille qu'à « ses » processus de rétablissement, mais globalement, il n'y a aucune vue d'ensemble de l'établissement. Les propositions d'adaptation d'EXPERTsuisse pour les Cm 79 et 80 sont elles aussi reprises.

En ce qui concerne les externalisations, les attentes fondamentales sont mentionnées dans la Circ.-FINMA 18/3. La nouvelle circulaire intègre des précisions sur le BCM ainsi que le DRP qui n'apparaissent pas avec une telle clarté dans la Circ.-FINMA 18/3 et, selon l'expérience historique, sont souvent omises. Par conséquent, la FINMA estime qu'un renvoi explicite aux dépendances externes reste pertinent.

Conclusion

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec le BCM sont désormais synthétisées dans le chapitre consacré à la gestion globale des risques opérationnels. Le terme d'« exercices » est introduit comme exemple de tests de mise en œuvre du BCP et du DRP. La fréquence minimale de test des processus critiques pour les établissements des catégories 1 à 3 est conservée. L'approbation de la stratégie pour le BCM doit être régulièrement demandée et le compte rendu effectué au moins une fois par année. Le traitement des scénarios graves mais plausibles dans le BCM est conservé. Il est clarifié qu'il faut au moins un DRP, c.-à-d. qu'il peut aussi en exister plusieurs. La nouvelle circulaire précise que les BIA, BCP et DRP doivent être contrôlés et adaptés si nécessaire au moins une fois par année mais aussi ad hoc en cas de changements importants. Le traitement de thèmes d'externalisation isolés est conservé.

3.11 Résilience opérationnelle et annexe 1

3.11.1 Délimitations et dépendances (Cm 45, 76, 93 et 94 ainsi que Circ.-FINMA 18/3)

Prises de position

L'ASB et l'UBCS relèvent en lien avec le Cm 89 et 93 que la BIA selon le Cm 76 contient déjà une identification des incidents qui peuvent déclencher les plans. Selon l'ASB, il faudrait aussi préciser la délimitation entre l'inventaire des fonctions critiques (Cm 94) et l'inventaire des données critiques (Cm 45).

Un autre participant de l'audition demande de clarifier si les externalisations qui sont pertinentes pour la réalisation des fonctions critiques entrent automatiquement dans les externalisations des fonctions importantes selon la

Circ.-FINMA 18/3. La terminologie devrait être uniforme sur le plan international. Il existe actuellement plusieurs termes pour représenter la matérialité comme *critical*, *important* ou *material* en particulier.

Appréciation

Comme le BCM soutient la résilience opérationnelle, il est pertinent de s'inspirer des expériences acquises dans les BIA (Cm 76) ou de s'appuyer sur elles lorsqu'il en va de l'identification des menaces et des vulnérabilités des fonctions critiques (Cm 93). Toutefois, la FINMA considère qu'il est utile de conserver les deux chiffres marginaux car il ne s'agit pas d'une duplication. En outre, il n'existe pas de recouvrement à l'identique entre l'inventaire des composantes TIC (Cm 45) et l'inventaire des fonctions critiques (Cm 94) car les deux remplissent des objectifs différents. Toutefois, la FINMA part du principe que l'inventaire des TIC représente dans la pratique une source d'informations importante pour répertorier les fonctions critiques. En ce qui concerne les données critiques, la FINMA s'abstient délibérément d'introduire un automatisme selon lequel les données pertinentes pour les fonctions critiques sont automatiquement des données critiques, ou à l'inverse que les données critiques sont uniquement les données qui sont nécessaires pour réaliser les fonctions critiques. Cela serait réducteur et pourrait conduire à l'omission de risques importants.

De plus, la FINMA renonce délibérément à créer un automatisme selon lequel les externalisations pertinentes pour les fonctions critiques doivent automatiquement être aussi des externalisations importantes selon la Circ.-FINMA 18/3. Cela sera sans doute souvent le cas, mais il existe aussi des contre-exemples. Il peut arriver notamment que certaines externalisations qui globalement ne sont pas considérées comme des externalisations de fonctions importantes au sens de la Circ.-FINMA 18/3 (par ex. livraisons physiques d'argent et approvisionnement de distributeurs automatiques) sont cependant pertinentes pour la réalisation des fonctions critiques (par ex. trafic des paiements).

La FINMA demeure ouverte à l'usage de différents termes pour représenter la matérialité (critique, matériel, significatif, etc.). Il n'est par ex. par indispensable qu'un établissement qualifie ses fonctions critiques de « fonctions critiques » dans ses documents. D'autres terminologies sont aussi admises, comme *important business services*, dans la mesure où elles couvrent les concepts sous-jacents de la circulaire.

Conclusion

Les Cm 45, 76, 93 et 94 ne sont pas adaptés pour affiner les délimitations.

3.11.2 Tests et gestion des scénarios graves mais plausibles

Prises de position

L'ASB remarque que la gestion des scénarios de longue durée (Cm 97) n'est possible qu'avec des travaux préparatoires et des garanties de l'État. Selon le scénario, il faudrait déclencher des plans de catastrophe à l'échelon supérieur, sur le plan sectoriel ou suisse.

Le test d'interruptions prolongées est considéré comme infaisable et non pertinent. Il s'agit de choisir des mesures de sensibilisation à bas seuil. Un autre participant de l'audition remarque qu'un nombre important et ingérable de scénarios peut potentiellement découler du Cm 97.

L'IIAS recommande de prescrire une fréquence minimale fixe pour les tests.

Appréciation

La FINMA reconnaît que les établissements ne sont pas en mesure de gérer chaque scénario grave mais plausible et que la question de la nécessité d'une implication de l'État peut, le cas échéant, se poser (par ex. pandémies, guerres, pénuries d'électricité durables). La FINMA s'attend toutefois à ce qu'au moins des travaux préparatoires ainsi que des réflexions aient lieu et que des mesures soient prises pour renforcer la résilience opérationnelle afin que les établissements soient préparés au mieux en cas de crises systémiques (qui font également partie des scénarios graves mais plausibles).

Le test d'interruptions de longue durée selon le Cm 97 a été mal compris. Il n'est bien sûr pas nécessaire d'arrêter l'utilisation de ressources fondamentales pendant plusieurs mois pour effectuer un tel test. Le principe connu du BCM, selon lequel les tests ne doivent pas menacer les activités de l'établissement, reste en vigueur. En lieu et place, un type de tests moins intensifs est envisagé ici, comme un exercice *table-top* ou une réflexion approfondie sur un scénario. Dans le cadre de ces tests, il y a lieu de réfléchir si les activités, processus, services et ressources nécessaires peuvent réellement être rétablis, et si oui dans quelle mesure, à l'aide des plans existants dans la fourchette de tolérance aux interruptions admise par la fonction critique. Le Cm 97 est adapté de sorte à mentionner en plus des exercices. Il clarifie également le fait qu'il existe des cas pour lesquels l'aide de l'État est nécessaire. Les scénarios avec les conséquences les plus graves sont généralement ceux qui perdurent. Par conséquent, la FINMA renonce à supprimer du Cm 97 les scénarios de longue durée.

Comme on part du principe que les tests ou les exercices comportent une certaine complexité (en particulier dans le cas des grands établissements ou les établissements de taille moyenne), la FINMA renonce à remplacer la fréquence de test « régulière » par une fréquence minimale (par ex. annuelle).

Cela devrait permettre d'éviter des tests de qualité insuffisante en raison des délais serrés.

Conclusion

La FINMA complète que certains scénarios ne peuvent, le cas échéant, pas être gérés sans implication de l'État (par ex. pandémies, guerres, pénuries d'électricité durables). Dans ce cas, l'établissement doit effectuer des travaux préparatoires pour renforcer sa résilience opérationnelle à l'égard de ces scénarios dans le cadre de ses possibilités. En outre, la FINMA précise que les tests peuvent aussi être effectués par des exercices et que les tests ou exercices doivent être conçus de sorte à ne pas menacer fondamentalement l'établissement.

3.11.3 Autres prises de position sur la résilience opérationnelle

L'UBCS demande que les banques de la catégorie 3 soient retirées du Cm 90 ou que l'organe responsable de la haute direction approuve les fonctions critiques et les tolérances aux interruptions non pas annuellement mais périodiquement ou en cas de changements importants.

Selon Clientis SA, le chapitre doit fusionner avec le chapitre sur le BCM.

EXPERTsuisse recommande d'énumérer en plus au Cm 91 les risques TIC ainsi que les cyberrisques et de demander un compte rendu selon le Cm 92 aussi en cas de changements importants dans l'activité de l'entreprise.

Credit Suisse demande si les risques opérationnels et les contrôles clés mentionnés au Cm 95 se réfèrent exclusivement à la poursuite des fonctions critiques. Un autre participant de l'audition remarque que la couverture demandée au Cm 96 des composantes des fonctions critiques par des BCP n'est pas suffisante pour garantir la résilience opérationnelle.

NCC Group recommande que *resilience by design* acquière une plus grande valeur. La demande en solutions *escrow* et la réglementation contractuelle avec des prestataires tiers en lien avec les exigences de test ainsi que les plans *exit* (en particulier *stressed exit*) seraient particulièrement pertinentes. Pour une meilleure compréhension des risques de concentration et des cyberrisques, il faut plus d'échange d'informations, en particulier en lien avec les audits anonymes des conventions d'externalisation, les évaluations d'externalisations non essentielles et les plans *business continuity* et *stressed exit* qui ont échoué et ont surtout été effectués par des prestataires importants.

En ce qui concerne les graphiques de l'annexe 1, l'UBCS recommande d'ajouter un texte explicatif alors que Clientis SA considère les graphiques comme peu pertinents et recommande de les supprimer.

Appréciation

Compte tenu de l'importance des établissements de la catégorie 3, de leur présence et de leur influence sur la place financière suisse ainsi que de leur portefeuille généralement considérable de clientes et clients, la FINMA considère que l'attention de l'organe responsable de la haute direction en lien avec les fonctions critiques est d'une telle pertinence qu'elle conserve la fréquence d'approbation annuelle.

Comme déjà mentionnée dans le rapport explicatif, la FINMA a examiné la possibilité d'un regroupement du BCM et de la résilience opérationnelle avant de la rejeter. En clair, le BCM définit les réactions aux interruptions (réactif ; réagissant aux interruptions) alors que la résilience opérationnelle vise fondamentalement une organisation déjà résiliente du modèle d'exploitation (préventif ; évitant les interruptions). Il s'agit par conséquent de concepts différents. Un regroupement enverrait un faux signal.

Conformément à la proposition d'EXPERTsuisse, la gestion des risques TIC et des cyberrisques est ajoutée au Cm 91 ; toutefois, un compte rendu annuel à l'intention de l'organe responsable de la haute direction est suffisant selon la FINMA.

En réponse à la question de Credit Suisse sur les risques opérationnels des fonctions critiques (Cm 95), la FINMA précise qu'il doit s'agir de risques opérationnels importants. Toutefois, cela n'inclut pas seulement les risques en lien avec la disponibilité. De plus, la définition du terme de résilience opérationnelle a été adaptée et complétée pour clarifier qu'il ne faut pas seulement des BCP pour garantir la résilience opérationnelle, comme cela est suggéré au Cm 96.

L'idée de la *resilience by design* était déjà incluse dans la définition de la résilience opérationnelle ; elle est désormais soulignée encore davantage. Le thème du *stressed exit* compte lui aussi une entrée explicite dans la circulaire. Par *stressed exit*, on entend le départ imprévu ou non ordonné d'un prestataire, par ex. pour cause d'insolvabilité, de sanctions ou de défaillance de ressources fondamentales nécessaires au prestataire.

Compte tenu des adaptations et des compléments apportés aux définitions du BCM et de la résilience opérationnelle, la FINMA considère que le graphique I de l'annexe 1 n'est plus nécessaire. Il est par conséquent supprimé.

Conclusion

La fréquence d'approbation annuelle est maintenue. La garantie de la résilience opérationnelle est traitée comme jusque-là dans un chapitre séparé. La définition de la résilience opérationnelle est adaptée et complétée. Les

termes de *resilience by design* et *stressed exit* sont mentionnés explicitement dans la circulaire. Le graphique I de l'annexe 1 est supprimé.

3.12 Maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique

Prises de position

Clientis SA propose d'intégrer le principe 8 concernant le maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique dans le principe 6 concernant le BCM.

Appréciation

Contrairement au principe 6, le principe 8 ne concerne que les banques d'importance systémique. Cela mis à part, les deux principes traitent de deux situations différentes : si la banque est en liquidation ou en assainissement, elle doit encore pouvoir fournir les fonctions d'importance systémique durant cette phase. Dans le BCM, par contre, il s'agit entre autres d'éviter d'en venir à une situation de liquidation ou d'assainissement.

Conclusion

Le maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique est traité séparément comme jusque-là.

3.13 Délais transitoires

Prises de position

L'ASB, l'UBCS, Clientis SA, EXPERTsuisse et l'IIAS ainsi qu'un autre participant estiment que les délais transitoires sont insuffisants.

L'ASB et l'UBCS recommandent par conséquent une prolongation des délais transitoires d'une année pour la résilience opérationnelle et un délai transitoire d'une année pour tous les autres principes. L'IIAS et un autre participant recommandent un délai transitoire d'au moins une année pour la gestion des risques des données critiques ; un autre participant demande un tel délai en plus pour la gestion des risques TIC. Clientis SA souhaite un délai transitoire global de deux ans.

Appréciation

La FINMA reconnaît le besoin des participants de prolonger les délais transitoires. Dans le cadre de ses commentaires et de son analyse des effets, la FINMA avait expliqué que si la circulaire procédait certes à des reformulations considérables dans certains principes, la pratique de surveillance sous-jacente ne changeait pas substantiellement. C'est notamment le cas dans la gestion des risques opérationnels, la gestion des cyberrisques et le BCM. En outre, les principes sur la gestion des risques liés aux services transfrontières et le maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique ont été repris tels quels de la Circ.-FINMA 08/21 à l'exception de quelques adaptations linguistiques mineures. Le concept des données critiques n'est pas non plus fondamentalement nouveau, car il fait déjà partie du principe 4 « Infrastructure technologique » de la Circ.-FINMA 08/21. Toutefois, la FINMA reconnaît que les reformulations opérées peuvent éveiller un besoin de clarification approfondi (par ex. évaluation des écarts de type *gap assessment* et élimination des lacunes éventuelles) auprès des assujettis.

Le délai transitoire pour la résilience opérationnelle, en revanche, n'est pas prolongé de trois à quatre ans car les trois ans ont été définis conformément aux délais transitoires des autorités de surveillance britanniques.

Conclusion

La date d'entrée en vigueur de la circulaire est reportée du 1er janvier 2023 au 1er janvier 2024 afin d'accorder suffisamment de temps aussi à la mise en œuvre des prescriptions en matière de gestion des risques opérationnels. Le délai transitoire jusqu'à la garantie de la résilience opérationnelle compte ensuite encore deux ans. En définitive, ce délai reste inchangé.

3.14 Activités d'audit

Prises de position

Selon l'IIAS, la couverture graduelle de la gestion des risques TIC pendant quatre ans, avec une étendue d'audit à définir librement par la société d'audit, n'est ni optimale ni cohérente par rapport à la couverture des thèmes apparentés, donc en particulier le BCM et la gestion des cyberrisques. Elle recommande d'harmoniser la couverture avec les autres domaines thématiques de la circulaire.

Appréciation

La couverture graduelle de la gestion des risques TIC a été choisie délibérément car il s'agit d'un vaste domaine thématique, souvent complexe, dont l'audit complet est généralement impossible en une année. Par conséquent,

l'audit est réparti comme jusque-là sur plusieurs années. Sur la base des résultats de l'évaluation ex post de la Circ.-FINMA 13/3, les cycles pluriannuels pourront toutefois encore être adaptés.

Conclusion

La stratégie d'audit pour la gestion des risques TIC n'est pas adaptée sur la base de l'audition.

4 Conséquences

Les précisions qui ont été apportées au projet au vu des informations reçues lors de l'audition ne changent pas l'évaluation de l'analyse des effets réalisée dans le rapport explicatif[3].

5 Suite de la procédure

La circulaire entièrement révisée « Risques et résilience opérationnels – banques » entrera en vigueur le 1er janvier 2024.

Des délais transitoires de deux ans à compter de l'entrée en vigueur s'appliquent à la garantie de la résilience opérationnelle. La garantie de la résilience opérationnelle doit ainsi être donnée jusqu'au 1er janvier 2026.

La Circ.-FINMA 13/3 partiellement révisée « Activités d'audit » entrera en vigueur le 1er janvier 2024.

[3] Concernant les conséquences, cf. rapport explicatif du 10 mai 2022, chapitre 7 « Analyse des effets », p. 29 ss.