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

Rapport explicatif

10 mai 2022

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

Table des matières

Éléments essentiels

1. La FINMA procède à une révision totale de sa circulaire 2008/21 « Risques opérationnels – banques ». Celle-ci sera remplacée par une nouvelle circulaire FINMA « Risques et résilience opérationnels – banques ».

2. Les modifications apportées aux exigences qualitatives qu'expose la Circ.-FINMA 08/21 se composent de concrétisations de la pratique de surveillance, d'une part en lien avec la gestion des risques opérationnels de manière générale, la gestion des risques liés à la technologie de l'information et de la communication (TIC) et aux données critiques ainsi qu'aux cyberrisques en particulier et d'autre part en lien avec le *business continuity management* (BCM) ainsi que la résilience opérationnelle.

3. Les modifications apportées aux exigences qualitatives reposent sur les « Revisions to the Principles for the Sound Management of Operational Risk » (PSMOR) et les nouveaux « Principles for Operational Resilience » (POR) du Comité de Bâle sur le contrôle bancaire (CBCB) publiés en mars 2021.

4. Les modifications apportées aux exigences qualitatives sont technologiquement neutres et fondées sur des principes. La proportionnalité est prise en compte de manière adéquate.

5. Les exigences en matière de fonds propres exposées dans la Circ.-FINMA 08/21 seront remplacées, dans le cadre de la mise en œuvre des règles finales de Bâle III, par les exigences découlant de l'ordonnance sur les fonds propres à réviser et par les dispositions d'exécution correspondantes de la FINMA. Par conséquent, elles ne font pas l'objet de la nouvelle circulaire.

6. La révision totale engendre des changements de la circulaire 2013/3 « Activités d'audit », laquelle sera en même temps partiellement révisée. La nouvelle Circ.-FINMA 08/21 et la Circ.-FINMA 13/3 partiellement révisée devraient entrer en vigueur le 1er janvier 2023 ; elles prévoient certains délais transitoires.

Liste des abréviations

ASB	Association suisse des banquiers
BCM	*Business continuity management*
BRP	*Business recovery plan*
CBCB	Comité de Bâle sur le contrôle bancaire
DDoS	*Distributed denial of service*
DRP	*Disaster recovery plan*
GDPR	*General data protection regulation* de l'Union européenne (UE)
LB	Loi fédérale du 8 novembre 1934 sur les banques (RS 952.0)
LEFin	Loi fédérale du 15 juin 2018 sur les établissements financiers (RS 954.1)
LFINMA	Loi fédérale du 22 juin 2007 sur la surveillance des marchés financiers (RS 956.1)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1)
LSFin	Loi fédérale du 15 juin 2018 sur les services financiers (RS 950.1)
OB	Ordonnance du 30 avril 2014 sur les banques (RS 952.02)
OEFin	Ordonnance du 6 novembre 2019 sur les établissements financiers (RS 954.11)
OFR	Ordonnance du 1er juin 2012 sur les fonds propres (RS 952.03)
OICV	Organisation internationale des commissions de valeurs
OLPD	Ordonnance du 14 juin 1993 relative à la protection des données (RS 235.11)
POR	« Principles for operational resilience » du CBCB du 31 mars 2021

PSMOR	« Revisions to the Principles for the Sound Management of Operational Risk » du CBCB du 31 mars 2021
RPO	*Recovery point objective*
RTO	*Recovery time objective*
TIC	Technologie de l’information et de la communication

1 Contenu et objectif du projet

La circulaire FINMA 2008/21 « Risques opérationnels – banques » (Circ.-FINMA 08/21) expose notamment les exigences qualitatives en matière de gestion des risques opérationnels. Par-là, elle concrétise les lois et les ordonnances du Conseil fédéral existantes (en particulier art. 3 al. 2 let. a et 3*f* LB, art. 12 OB, art. 9 LEFin et art. 68 OEFin) concernant l'organisation, la séparation des fonctions, la gestion des risques et le contrôle interne par rapport aux risques opérationnels.

Les nouveaux POR, les PSMOR révisés du CBCB ainsi que les fortes évolutions dans le domaine de la numérisation et de la TIC ont incité à une révision totale de la Circ.-FINMA 08/21.

L'objectif de la nouvelle circulaire « Risques et résilience opérationnels – banques » consiste à accroître la transparence sur l'application du droit des marchés financiers par la FINMA en matière de risques opérationnels et de résilience opérationnelle. La mise en œuvre est limitée à l'essentiel, fondée sur des principes, proportionnelle, technologiquement neutre et conforme aux normes internationales.

Les changements engendrés par la nouvelle circulaire sur les activités d'audit auprès des banques et des maisons de titres se feront à travers une révision partielle de la Circ.-FINMA 13/3 « Activités d'audit ».

2 Actions requises

La mise en œuvre des normes internationales, prévue à l'art. 7 al. 2 let. d LFINMA, fait partie de la stratégie des marchés financiers du Conseil fédéral. Elle comprend également les nouvelles prescriptions du CBCB.

Les prescriptions internationales suivantes du CBCB doivent être mises en œuvre dans le cadre de la présente révision totale :

- « Bâle III : finalisation des réformes de l'après-crise »[1], décembre 2017. Ce document contient une nouvelle méthode de calcul des fonds propres minimaux pour les risques opérationnels, qui est mise en œuvre au niveau de l'ordonnance. Par conséquent, les exigences en matière de fonds propres de la Circ.-FINMA 08/21 ne font plus partie de la nouvelle circulaire. La mise en œuvre des règles finales de Bâle III fait l'objet d'un processus séparé au niveau du Conseil fédéral (OFR) ainsi que de la FINMA (ordonnances d'exécution correspondantes). Le chapitre 8

[1] Disponible sur https://www.bis.org/bcbs/publ/d424.htm

expose notamment la suppression des exigences en matière de fonds propres ainsi que la réglementation transitoire.

- « Principles for Operational Resilience »[2] (POR), mars 2021. Il s'agit d'un nouveau document qui vise à renforcer la capacité de résistance opérationnelle (résilience) des banques face aux menaces accrues et plus complexes, en particulier en lien avec la numérisation croissante.

- « Revisions to the Principles for the Sound Management of Operational Risk »[3] (PSMOR), mars 2021. Il s'agit d'une révision des principes déjà existants visant à gérer les risques opérationnels. Le CBCB a examiné les principes existants en regard de leur adéquation permanente, les a mis à jour et complétés par un nouveau principe sur la TIC.

La nouvelle circulaire permet à la FINMA de clarifier la mise en œuvre de ces prescriptions internationales du CBCB sur la gestion des risques opérationnels et la résilience opérationnelle dans le cadre de la législation des marchés financiers. La circulaire sert exclusivement à l'application du droit et ne contient aucune disposition fixant des règles de droit.

Une mise à jour de la Circ.-FINMA 08/21 est par ailleurs indiquée pour tenir compte des évolutions importantes dans le domaine technologique qui sont intervenues depuis la publication de la circulaire. Les dépendances envers une TIC fonctionnant de manière irréprochable ont augmenté, alors que les systèmes TIC et les chaînes d'approvisionnement ont en général gagné en complexité, impliquant de nouvelles problématiques. De plus, les défaillances importantes ainsi que les cyberattaques sont devenues plus fréquentes. Faisant partie intégrante de ces évolutions, des défis en lien avec la gestion des données du point de vue de la confidentialité, de l'intégrité et de la disponibilité sont apparus plus clairement.

Les changements apportés à la Circ.-FINMA 08/21 rendent nécessaire une modification de la Circ.-FINMA 13/3 concernant l'audit des banques et des maisons de titres, laquelle modification comprendra notamment des adaptations relatives aux champs d'audit en lien avec la Circ.-FINMA 08/21.

3 Contextes national et international

La révision totale de la Circ.-FINMA 08/21 s'appuie sur les prescriptions des documents du CBCB cités au chapitre 2. En cas de disponibilité et de pertinence thématique, des modèles d'autres pays ont également été utilisés à des fins de comparaison.

[2] Disponible sur https://www.bis.org/bcbs/publ/d516.htm

[3] Disponible sur https://www.bis.org/bcbs/publ/d515.htm

La résilience opérationnelle ainsi que les risques TIC et les cyberrisques sont devenus des thèmes prioritaires internationaux déjà avant la pandémie de coronavirus. Celle-ci n'a fait que renforcer leur importance et leur urgence. De nombreuses autorités d'autres pays, en particulier dans le domaine de la surveillance des marchés financiers, ont par conséquent émis dans l'intervalle de nouvelles prescriptions ou des prescriptions révisées. Les autorités britanniques, par ex., ont élaboré depuis 2018 divers documents sur la garantie de la résilience opérationnelle. Les autorités américaines ont publié en novembre 2020 leur « U.S. Interagency Paper on Sound Practices to Strengthen Operational Resilience ». L'Union européenne prépare le « Digital Operational Resilience Act » et l'OICV un document sur la résilience opérationnelle des plates-formes de négociation et des intermédiaires de marché.

La mise en œuvre des documents du CBCB cités au chapitre 2 a nécessité notamment une mise à jour des informations pour le BCM. La Circ.-FINMA 08/21 ne comprenait à cet égard qu'un seul chiffre marginal, car certains chapitres des « Recommandations de l'ASB en matière de Business Continuity Management (BCM) » d'août 2013 étaient simultanément reconnus comme autorégulation selon l'art. 7 al. 3 LFINMA. Sur demande de la FINMA, l'ASB a consulté en 2021 ses banques membres et est parvenue à la conclusion qu'à l'avenir un traitement exclusif du thème dans la nouvelle circulaire serait à privilégier et qu'il faudrait renoncer à une actualisation des recommandations existantes. Les passages desdites recommandations de l'ASB reconnus comme autorégulation sont désormais couverts par la nouvelle circulaire et la reconnaissance de l'autorégulation mentionnée en tant que standard minimal sera supprimée à l'entrée en vigueur de la nouvelle circulaire.

4 Commentaires des dispositions

4.1 Circulaire FINMA « Risques et résilience opérationnels – banques »

4.1.1 Remarques préliminaires

La gestion des risques opérationnels décrite dans la nouvelle circulaire fait partie intégrante de la gestion des risques à l'échelle de l'établissement selon la Circ.-FINMA 17/1 « Gouvernance d'entreprise – banques » (Circ.-FINMA 17/1). Elle doit par conséquent s'intégrer dans la gestion des risques à l'échelle de l'établissement.

La gestion des risques opérationnels est globale et comprend notamment les risques juridiques et de *compliance*, les risques TIC et les cyberrisques, les risques associés à des données critiques ou les risques d'interruption.

Les exigences envers la gestion des risques opérationnels constituent le principe 1 de la circulaire. Les principes 2 à 5 sur les risques TIC, les cyber-risques, les risques liés aux données critiques et les risques liés aux activités de service transfrontières concrétisent les exigences posées par la gestion de ces risques spécifiques. La nouvelle circulaire n'a pas pour ambition de traiter de manière globale ou en détail tout type de risque opérationnel. Spécialement en matière de risque juridique, le droit applicable doit être identifié et respecté dans tous les cas, par ex. en lien avec le risque de blanchiment d'argent ou la protection des données.

Les principes 6 et 7 sur le BCM et la résilience opérationnelle concrétisent les exigences envers les procédures liées au risque d'interruption. Alors que le BCM traite du rétablissement spécifique de l'activité en cas d'interruption, la résilience opérationnelle se réfère à l'identification et au renforcement stratégiques des fonctions importantes pour l'établissement et la place financière, c.-à-d. les « fonctions critiques ». La résilience opérationnelle repose sur le BCM et une gestion solide des risques opérationnels.

Tous les principes concernant les exigences qualitatives de la Circ.-FINMA 08/21 ont été examinés et adaptés. Les principes 6 (désormais 8) et 7 (désormais 5) ont par conséquent été repris presque tels quels dans la nouvelle circulaire.

Le principe de proportionnalité s'applique dans toute la circulaire, c.-à-d. que les chiffres marginaux doivent être mis en œuvre en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement. De plus, certains chiffres marginaux ne s'appliquent pas aux banques et maisons de titres des catégories FINMA 4 et 5 ainsi qu'aux établissements participant au régime des petites banques et les maisons de titres qui ne gèrent pas de comptes. Ces établissements bénéficient dès lors de plus de flexibilité en matière d'organisation et de mise en œuvre.

Comme la circulaire est technologiquement neutre et fondée sur des principes, elle renonce délibérément à aborder les particularités de technologies spécifiques comme la gestion des externalisations dans le *cloud*.

4.1.2 Principe 1 : exigences générales en matière de gestion des risques opérationnels (Cm 20 à 34)

Le principe 1 comprend une révision des principes 1 à 3 de la Circ.-FINMA 08/21 sur les thèmes « catégorisation et classification des risques opérationnels », « identification, limitation et surveillance » ainsi que « établissement de rapports internes et externes ». Il expose dès lors les composantes fondamentales garantes d'une gestion efficace des risques opérationnels.

Les orientations suivantes ont inspiré la révision :

- Comparaison et mise à jour par rapport aux PSMOR révisés : comme la révision du document du CBCB s'est produite sur le plan granulaire, son influence sur la gestion générale des risques opérationnels dans la nouvelle circulaire s'est révélée secondaire. Le principe sur la TIC nouvellement introduit dans le document du CBCB est plus pertinent pour la nouvelle circulaire et a été pris en compte dans les principes 2 à 4.
- Mise à jour et clarification sur la base des expériences issues de la pratique de surveillance de la FINMA : la révision vise avant tout à remédier aux erreurs d'interprétation et aux lacunes dans le domaine de la gestion des risques opérationnels qui ont souvent été constatées dans la pratique. Comme expliqué ci-après, elle clarifie en particulier la pratique de surveillance sur la tolérance au risque s'agissant des risques opérationnels (Cm 22, 29, 31). De plus, les contrôles clés sont considérés comme composante essentielle du système de contrôle interne (Cm 28). Le lien avec la gestion des risques à l'échelle de l'établissement selon la Circ.-FINMA 17/1 est précisé plus clairement (Cm 20 à 23).

La définition des risques opérationnels (Cm 3) reste identique sur le fond et s'aligne sur celle du CBCB et de l'OFR. Comme mentionné déjà au chapitre 4.1.1 les risques opérationnels incluent de nombreux types de risques, dont notamment les risques de *compliance* (par ex. risques de blanchiment d'argent, risques découlant des exigences en matière de *suitability* et *appropriateness*), le risque de fraude, de cyberattaque ou d'interruption, ainsi que les risques juridiques comme le risque d'une action en justice.

La définition des risques opérationnels ne comprend pas les risques stratégiques (par ex. le risque que l'offre d'un nouveau produit ne génère pas les résultats souhaités et attendus). Elle exclut aussi les risques de réputation, bien qu'ils soient étroitement apparentés aux risques opérationnels et qu'une séparation nette soit rarement possible. Les incidents ou les pertes découlant des risques opérationnels se répercutent ainsi souvent sur la réputation de l'établissement. Si la culture de l'établissement se révèle déficiente, il peut en découler des risques de comportement (appartenant aux risques opérationnels), qui peuvent se matérialiser par des conduites fautives de collaborateurs. Si ces comportements parviennent à l'attention des médias, ils entachent la réputation de l'établissement. Celle-ci peut également être pénalisée par une cyberattaque qui, en perturbant l'activité commerciale de l'établissement, suscite l'intérêt des médias et affecte la clientèle.

La gestion des risques opérationnels est à comprendre au sens de composante de la gestion des risques à l'échelle de l'établissement selon la Circ.-FINMA 17/1 (Cm 20). La séparation des fonctions décrite dans la Circ.-FINMA 17/1 est à mettre en œuvre ici aussi en appliquant le principe de proportionnalité. C'est la raison pour laquelle la nouvelle circulaire n'entre

pas dans les détails de cette séparation entre fonctions (souvent appelées la 1re et la 2e lignes de défense) dans le contexte de la gestion des risques opérationnels.

Le rôle et la responsabilité de l'organe responsable de la haute direction présentés dans la Circ.-FINMA 17/1 sont précisés dans la nouvelle circulaire en lien avec les risques opérationnels. Une présentation transparente et actuelle des risques inhérents et résiduels de l'établissement doit être soumise à l'organe responsable de la haute direction, à partir de laquelle celui-ci définit et approuve la tolérance au risque (Cm 22).

Alors que la réaction aux risques (prévention, transfert, réduction, acceptation) et les mesures à prendre peuvent être décidées en détail à l'échelle de la direction ou des unités opérationnelles, l'organe responsable de la haute direction est compétent pour décider des changements stratégiques de direction s'il considère que certains risques inhérents ou résiduels ne sont pas ou plus tolérables. Les changements stratégiques de direction peuvent consister notamment à modifier le modèle d'affaires (par ex. renoncer aux activités transfrontières ou à des opérations dans certains pays, renoncer à certains produits, à l'*investment banking* ou à certains groupes clientèle cibles) ou à adapter soit le modèle organisationnel soit le mode opératoire (par ex. forte réorientation vers l'automatisation et la réduction des processus manuels ou nouvelles externalisations de services essentiels).

Lors des évaluations des risques et des contrôles, toutes les informations pertinentes doivent être prises en compte (Cm 27). En outre, les responsables ne doivent pas se fier exclusivement aux données « réactives » lors de l'évaluation des mesures de contrôle et d'atténuation (Cm 28). Par ex. celles-ci ne devraient pas être considérées comme efficaces simplement parce qu'aucun événement (de perte) n'a été enregistré au cours des dernières années. En lieu et place, il s'agit au minimum de tester régulièrement et systématiquement les contrôles clés et d'intégrer les résultats de ces tests. En ce qui concerne les tests des contrôles clés, il est important que ceux-ci soient testés périodiquement, au moins par échantillonnage, par une unité organisationnelle indépendante telle que le contrôle des risques ou la révision interne (voir également la Circ.-FINMA 17/1), en complément des évaluations effectuées par les unités organisationnelles qui définissent, « possèdent » et exécutent les contrôles clés (*control owners* et *control performers*).

En cas de changements importants, l'évaluation des risques et des contrôles doit être actualisée (Cm 29). On entend par changements importants par ex. la migration vers un autre système IT doté de nouvelles procédures, les procédures modifiées, l'introduction ou la suppression de produits, l'introduction ou l'abandon de certaines activités commerciales, les changements dans les groupes de clientèle cibles (par ex. autre pays, autre type de clientèle), l'entrée en vigueur de nouvelles réglementations ou les menaces accrues.

Le rapport interne sur les risques opérationnels doit notamment comprendre des informations sur les pertes internes importantes dues aux risques opérationnels (Cm 32). Cela ne signifie pas que chaque établissement doive nécessairement mettre en œuvre une collecte systématique des données sur les pertes conformément au Cm 30 ou aux exigences relatives aux données internes sur les pertes pour le calcul des fonds propres minimaux pour les risques opérationnels selon les règles finales de Bâle III. Une collecte systématique des données sur les pertes est certes recommandée, mais n'est pas attendue de chaque établissement en application du principe de proportionnalité.

4.1.3 Principe 2 : gestion des risques TIC (Cm 35 à 52)

Les risques TIC constituent un type spécifique de risques opérationnels. Sur la base des exigences générales établies dans le principe 1, le principe 2 fournit des indications détaillées sur la gestion des risques TIC.

Pour des questions de lisibilité, les principes en matière de gestion des risques TIC, des cyberrisques et des risques liés aux données critiques renoncent à se référer explicitement à la circulaire FINMA 2018/3 « Outsourcing » et à la Circ.-FINMA 17/1. Toutefois, leurs principes restent en vigueur. Il s'agit en particulier d'appliquer les exigences à l'égard des structures organisationnelles, de la politique des risques et des grandes lignes en matière de gestion des risques à l'échelle de l'établissement selon la Circ.-FINMA 17/1.

La nouvelle circulaire précise en particulier les différentes responsabilités de l'organe responsable de la haute direction (accent mis sur l'approbation et la surveillance) et de la direction (accent mis sur la mise en œuvre) dans les domaines de la stratégie TIC, de la gestion des risques TIC ainsi que de la garantie des principes de confidentialité, d'intégrité et de disponibilité des TIC (Cm 35, 39 et 41).

La TIC représente une composante essentielle de l'activité des établissements. Ceux-ci doivent par conséquent développer et mettre en œuvre un système approprié de gestion des risques TIC en tenant compte de leur taille, de leur complexité, de leur structure et de leur profil de risque. Au sein des établissements, la gestion de ces risques nécessite des connaissances spécialisées adéquates de la part des membres de la direction et de l'organe responsable de la haute direction. Les processus et procédures en matière de contrôle des risques TIC doivent aussi, en accord avec les conditions spécifiques de l'établissement, tenir compte des normes générales reconnues sur le plan international (Cm 36 et 37).

La gestion des changements *(change management)* a pris de l'importance compte tenu des évolutions importantes dans le domaine des TIC, à l'instar de la méthode « Agile » (Cm 42 à 44). La circulaire met l'accent sur le

change management pour traiter tout type de changement *(change)* apporté à une infrastructure TIC. Un processus de *change management* structuré, bien défini et contrôlé permet la mise en œuvre efficace des changements et contribue de ce fait à la diminution des risques. Ce faisant, les répercussions des changements formulés par le biais d'un *change request* doivent être déterminées et les modifications qui en découlent doivent être classifiées et priorisées. Le processus de *change management* inclut en règle générale les activités suivantes : réception, classification, approbation[4], autorisation, planification, test et validation du test ainsi que le déploiement dans l'environnement de production. La collaboration étroite entre les disciplines *change management*, gestion des projets et *release management* est un facteur déterminant pour mettre en œuvre efficacement le *change management*.

Pour prévenir tout accès non autorisé, la circulaire met en avant la séparation entre les environnements de production et les environnements de test ou de développement (Cm 43). Pour ce faire, l'établissement doit garantir la séparation des tâches à l'aide de procédures, de processus et de contrôles appropriés. Les *code-reviews*, la validation d'artéfacts (*« build »)* par un *product owner*, les tests intégrés et indépendants ou les mécanismes d'enregistrement d'évènements (*« logging »)* peuvent être utilisés à cet effet. Généralement, la séparation des fonctions représente le contrôle préventif le plus important en vue de se protéger des accès non autorisés dans l'environnement de production. Compte tenu de la diffusion croissante de méthodes de développement flexibles de type agile, la circulaire renonce toutefois à nommer la séparation des fonctions comme standard minimal. De plus, celle-ci serait souvent irréalisable dans les très petits établissements qui misent, en lieu et place, sur des contrôles compensatoires.

Une exploitation TIC structurée bien définie et contrôlée *(run, maintenance)* garantit la confidentialité, l'intégrité et la disponibilité de l'environnement de production TIC (Cm 45 à 49). Plus l'environnement TIC d'un établissement est complexe, plus la maîtrise du risque de la fin de vie des composantes de l'infrastructure TIC *(end of life)* et leur prise en charge par le fabricant est difficile. Par conséquent, les établissements sont tenus de garantir une gestion contrôlée et orientée sur les risques des systèmes dont la fin de l'exploitation approche ou dont la mise hors service n'a pas été effectuée comme prévu.

La circulaire précise l'importance fondamentale de posséder un inventaire TIC qui inclut les composants matériels et logiciels ainsi que les données critiques (Cm 45). L'inventaire TIC doit tenir compte des dépendances internes ainsi que des interfaces avec les prestataires externes essentiels. Celui-ci doit permettre une évaluation structurée des éléments TIC physiques et virtuels, à disposition d'un établissement. L'existence d'informations actuelles et exhaustives issues de l'inventaire TIC est primordiale à la

[4] Généralement par un organe tel que le *change review board* ou une autre *change authority*.

gestion des changements ainsi qu'à la réaction rapide aux incidents TIC et aux cyberincidents, ainsi qu'en cas de problèmes liés à un système IT déterminé ou d'achats futurs destinés à la maintenance et à l'extension de l'exploitation (Cm 46 et 55). De plus, l'inventaire TIC constitue le fondement des évaluations visant à déterminer si les éléments de l'infrastructure TIC ne fonctionnent pas selon les attentes ou n'étant plus standards doivent être reconfigurés *(patching)*, échangés ou complètement mis hors service.

L'exploitation TIC n'est pas isolée ; elle doit être considérée en étroite relation avec les aspects de continuité des activités de type BCM et DRP (principe 6). Les établissements doivent garantir des transitions consistantes entre la gestion opérationnelle TIC et les procédures BCM ou DRP, qui sont à même de maintenir l'exploitation en cas d'interruption et de situation de crise (Cm 48). Cela signifie que les processus correspondants de sauvegarde et de restauration doivent être testés au moins une fois par année. Dans ce cadre, il s'agit également de tester les mécanismes de sécurité qui détectent et limitent les risques de restauration erronés ainsi que les éventuelles données corrompues.

La circulaire précise également les grandes lignes de la gestion des incidents TIC (*incident management*, Cm 50 à 52). La gestion des incidents englobe l'ensemble du processus organisationnel et technique relatif à la gestion des défaillances opérationnelles connues ou supposées ainsi que les incidents ayant trait à la sécurité dans les domaines TIC, y compris les mesures et les processus préparatoires de réaction et d'escalade. Afin de tirer des conclusions et des leçons d'incidents antérieurs, elle doit tenir compte de l'ensemble du cycle de vie des incidents TIC.

4.1.4 Principe 3 : gestion des cyberrisques (Cm 53 à 58)

Les cyberrisques font partie des risques opérationnels qui sont traités de manière générale dans le principe 1.

Le principe 3, quant à lui, précise les exigences en matière de gestion appropriée des cyberrisques. Les cyberrisques sont étroitement liés aux risques TIC du principe 2, car la matérialisation des risques TIC peut aboutir à une augmentation des cyberrisques et inversement. Toutefois, les cyberrisques ne peuvent pas être assimilés à des risques TIC. Ils sont soumis à des facteurs d'influence externes plus forts comme l'exploitation des faiblesses via différents vecteurs d'attaques, tels que les logiciels de rançon (*ransomware)*, les attaques par déni de service distribué *(distributed denial of service,* DDoS) et les menaces internes *(insider threat)*. Les établissements doivent par conséquent disposer, dans leur gestion des risques, de leur propre définition des cyberrisques, qui répond à la nature du risque pour leur établissement.

La révision des exigences en matière de cybersécurité dans la nouvelle circulaire s'appuie pour l'essentiel sur les expériences issues de la pratique de surveillance de la FINMA. Pour traiter efficacement les cyberrisques, les établissements devraient mettre en place leur SCI selon un standard international reconnu et les bonnes pratiques (Cm 55), comme le dispositif sur les cyberrisques du *National Institute of Standards and Technology* (NIST) ou les standards correspondants de l'Organisation internationale de normalisation (ISO). Ils doivent également rendre compte annuellement à la direction des évolutions du profil de menace et de risque, des éventuels dommages en cas de cyberattaque aboutie ainsi que garantir l'efficacité opérationnelle des contrôles clés dans ce domaine (Cm 54).

Les mesures à mettre en œuvre ont été précisées, afin de suivre une approche globale (Cm 55). Lors de l'identification des cyberattaques, l'accent a été mis sur l'introduction de procédures et de contrôles appropriés permettant de procéder à un inventaire global des TIC, dans l'objectif de garantir l'identification rapide de faiblesses et, dans le cas d'une cyberattaque, d'analyser et de bloquer plus rapidement les interconnexions. Cela comprend aussi l'implémentation appropriée de procédures, de processus et de contrôles visant à identifier, endiguer et écarter les cyberattaques de ce type.

Pour examiner l'efficacité des mesures de cyberprotection mises en œuvre, la direction doit mettre sur pied, outre une analyse des faiblesses et des tests d'intrusion, des cyberexercices sur la base du potentiel de menace spécifique à l'établissement (Cm 58). À titre complémentaire, il est possible d'exécuter d'autres procédures, qui ne figurent pas explicitement dans la circulaire, visant à examiner les mesures de cyberprotection, comme la participation à des programmes de prime au bug *(bug bounty)* ou des contrôles de sécurité des codes sources.

Le principe 3 décrit également l'obligation d'annoncer les cyberattaques à la FINMA (Cm 56). Les détails concernant le processus d'annonce ont été définis dans la communication sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA ».

4.1.5 Principe 4 : gestion des risques des données critiques (Cm 59 à 70)

Les nouvelles technologies et la numérisation induisent des changements fondamentaux dans le secteur financier. La qualité, l'intégrité, la sécurité et l'utilisation des données sont de plus en plus décisives pour l'orientation stratégique des établissements. La révision de la circulaire tient compte de ce fait en élargissant l'accent, qui était mis jusque-là sur la confidentialité relative aux données d'identification de la clientèle, aux dimensions d'intégrité et de disponibilité des données critiques dans un sens général.

Les données critiques sont des données qui doivent bénéficier d'une protection particulière et, par conséquent, être définies par l'établissement sur la base des risques (Cm 7). Elles peuvent être critiques tant du point de vue de la confidentialité que de l'intégrité ou de la disponibilité et sont soumises de ce fait à différents degrés de criticité :

- Les données critiques en matière de confidentialité, c.-à-d. les données confidentielles, sont des informations commerciales, des données liées à des clients ou à des personnes, qui doivent être protégées contre l'accès non autorisé afin de préserver la sphère privée ou la sécurité d'un individu ou d'une organisation.

- Les données critiques en matière d'intégrité et de disponibilité doivent être définies par l'établissement sur la base des risques. La criticité de ces données se réfère à la capacité de l'établissement de travailler avec efficacité et efficience, voire dans certains cas juste de travailler. Les données critiques sont dès lors vitales pour le fonctionnement de l'établissement (« données vitales »). Les données vitales sont par ex. des données qui sont utilisées dans des rapports financiers (tant internes qu'externes), des rapports réglementaires, pour un processus décisionnel, une réalisation technique ou mesurer la performance de l'entreprise. Quand des données de ce type sont endommagées, détruites ou inaccessibles, l'établissement, ses unités et son personnel ne peuvent potentiellement plus effectuer leurs tâches.

Les établissements doivent respecter leurs autres obligations légales, comme celles posées par le droit de la protection des données. La FINMA n'est pas compétente pour appliquer le droit de la protection des données.

En vertu du droit applicable en matière de protection des données (par ex. la LPD révisée), les établissements peuvent également être tenus de déclarer un incident au préposé à la protection des données compétent, ce qu'ils doivent faire en plus de leur obligation de déclaration à la FINMA. La compétence de surveillance du préposé à la protection des données dans le domaine de la protection des données reste inchangée.

Cette précision concernant la gestion des données critiques va aussi de pair avec un relèvement du niveau de protection que visait l'annexe 3 de la Circ.-FINMA 08/21. Cela comprend les éléments suivants :

- les obligations et les responsabilités de la direction et de l'organe responsable de la haute direction (Cm 59 et 60) ;

- la définition et la mise en œuvre par les établissements d'une stratégie en matière de données, qui compte notamment la définition de la stratégie, la gouvernance et l'organisation, les procédures, l'architecture des

données et de l'information ainsi que la protection des données (Cm 59) ;

- pendant le développement, le changement et la migration de systèmes, les données critiques doivent être protégées de manière adéquate contre l'accès et l'utilisation par des personnes non autorisées (Cm 64) ;

- l'évaluation des risques ne se traduit pas automatiquement par une protection élevée des structures d'autorisation. Par conséquent, la TIC physique et logique qui sauvegarde ou traite les données critiques est à protéger en particulier (Cm 65).

Les données critiques sont gérées tout au long de leur cycle de vie. Le cycle de vie comprend la responsabilité des données, la collecte des données, le lieu de stockage, l'entretien, la conservation (*retention*), la suppression et l'élimination. Il tient compte des aspects liés à la production, à l'enrichissement, au traitement et au transfert des données critiques.

Même si les établissements externalisent toujours plus leurs données et leurs processus IT à des prestataires non soumis à la surveillance de la FINMA, ils restent responsables de la gestion des risques, de la sécurité des données et du respect des lois et des prescriptions. Ces aspects sont traités dans la Circ.-FINMA 18/3. De ce fait, la nouvelle circulaire ne limite ni la mise en œuvre ni l'utilisation des solutions *cloud* ou d'autres technologies, mais stipule que les données doivent être protégées en conséquence en fonction de leur classification et des degrés de criticité définis par l'établissement.

4.1.6 Principe 5 : gestion des risques liés aux activités de service transfrontières (Cm 71 à 74)

La notion de « services financiers » a été remplacée par « services », car sa définition à l'art. 3 let. c LSFin est si étroite que certains services bancaires courants (dépôt ou prestations de paiement) ne seraient pas inclus. Hormis ce point terminologique, aucune modification n'a été effectuée.

4.1.7 Principe 6 : *business continuity management* (BCM ; Cm 75 à 88)

Ce principe révise l'ancien principe 5 « continuité en cas d'interruption de l'activité » de la Circ.-FINMA 08/21. Il consiste pour l'essentiel en une version actualisée, fondée sur des principes et conforme aux documents du CBCB, des « Recommandations de l'ASB en matière de Business Continuity Management (BCM) ». À cet égard, il est fait référence au chapitre 3.

Le BCM vise à garantir la réalisation des objectifs commerciaux même en cas d'interruption significative des processus critiques[5] (Cm 8). Il ne sous-entend pas obligatoirement l'existence de processus critiques dans chaque domaine commercial et organisationnel (Cm 76).

L'actualisation liée aux PSMOR du CBCB concerne la transparence sur les ressources nécessaires aux processus critiques ainsi que les relations et les interdépendances entre les ressources et les processus (Cm 76). Les quatre catégories[6] mentionnées dans les recommandations de l'ASB sont potentiellement restrictives. Par ex., les PSMOR nomment aussi les dépendances envers les banques centrales et les chambres de compensation. C'est la raison pour laquelle la nouvelle circulaire renonce à une énumération de ces quatre catégories. Une vue d'ensemble des ressources potentiellement nécessaires est fournie au chapitre 4.1.8. Au minimum les processus critiques indispensables aux fonctions critiques (cf. chapitre 4.1.8) réclament une compréhension plus large et détaillée que la compréhension demandée jusqu'alors concernant les ressources nécessaires.

De manière analogue, les tests se réfèrent désormais à des « scénarios graves mais plausibles » (Cm 86), afin d'empêcher la concentration sur des défaillances ponctuelles ou des défaillances de ressources isolées issues d'une des quatre catégories en vigueur. De plus, l'utilisation de cette terminologie vise à établir un lien avec le chapitre 4.1.8, car le BCM est l'une des composantes destinées à garantir la résilience opérationnelle.

Selon la taille et la complexité de l'établissement, il peut exister un *business continuity pla*n (BCP) à l'échelle de l'entreprise ou plusieurs BCP (Cm 11, 79).

En fonction de l'organisation de l'établissement, le *disaster recovery plan* (DRP)[7] peut être soit intégré dans le BCP soit saisi séparément. Toutefois, il fonctionne dans tous les cas comme partie de BCP. En d'autres termes, les précisions de la nouvelle circulaire liées au BCP s'appliquent aussi au DRP (Cm 12, 80).

La stratégie BCM d'un établissement définit sa procédure fondamentale en matière de BCM (Cm 9, 75). Elle définit le cadre nécessaire aux composantes du BCM et contient les options de rétablissement sélectionnées, qui sont détaillées dans le ou les BCP.

[5] Cela comprend les objectifs définis jusque-là dans les « Recommandations de l'ASB en matière de Business Continuity Management (BCM) » d'août 2013 visant à maintenir le service à la clientèle, respecter les obligations réglementaires de l'entreprise et/ou gérer les positions à risques pour éviter les dommages critiques (directs ou indirects) (cf. définition des « processus critiques » dans le glossaire des recommandations de l'ASB).

[6] Défaillance du personnel, défaillance des locaux, défaillance des systèmes informatiques ou de l'infrastructure informatique (y compris les systèmes de communication), défaillance de prestataires et de fournisseurs externes (externalisation) par ex. dans le domaine des fournisseurs d'information.

[7] Parfois appelé aussi *business recovery plan* (BRP).

Dans le domaine des TIC, ces éventuelles options de rétablissement englobent par ex. une solution *hot site, cold site* ou *warm site*. Elles se caractérisent généralement par différents coûts, fonctions et durées de rétablissement. L'évaluation des durées de disponibilité attendues est comparée avec les ressources indiquées dans les options de rétablissement et leur RTO.

Les formations et les mesures correspondantes sur le BCM sont, si nécessaire, adaptées aux groupes d'intérêt et régulièrement actualisées (Cm 88).

En cas d'apparition d'une situation de crise, le BCM, ou l'activation de l'état-major de crise, requiert l'attention complète et l'engagement total de la direction et de l'organe responsable de la haute direction (Cm 81). Par situation de crise, on entend par ex. les catastrophes et les événements naturels, une pandémie, les cyberattaques ciblées ou les interruptions complètes et de longue durée des TIC. Il importe que l'établissement ait déjà réglé au préalable la manière de gérer les situations de crise (déclencheur, état-major de crise, organisation de crise).

Pour les situations de crise, il convient également de définir une stratégie de communication (Cm 82). Celle-ci établit quel type de communication est requis pour quels groupes d'intérêt internes et externes (par ex. information aux collaborateurs, clients, contreparties et prestataires, communiqués de presse ainsi qu'obligation d'annonce à l'autorité de surveillance).

4.1.8 Principe 7 : résilience opérationnelle (Cm 89 à 98)

Depuis la crise financière 2007-2009, le CBCB a procédé à des réformes afin de renforcer la résilience financière des banques. Tandis que ses exigences en matière de fonds propres et de liquidité ont amélioré la capacité des banques à absorber les chocs financiers, la résilience opérationnelle n'a pas encore été suffisamment prise en compte jusque-là. On entend ici la capacité de résister aux chocs opérationnels significatifs avec le moins de conséquences négatives possibles, et de les surmonter rapidement. Les chocs opérationnels proviennent par ex. d'événements tels que des pandémies, des cyberattaques, des défaillances systémiques, des pannes dans les chaînes d'approvisionnement, des coupures d'électricité étendues ou durables, ou encore des catastrophes naturelles. La probabilité et les conséquences de tels événements ont augmenté ces dernières années.

Le BCM est un concept parmi d'autres à soutenir la résilience opérationnelle. Toutefois, ce dernier est encore jugé globalement insuffisant, car il met l'accent sur les plans de rétablissement consécutifs à une interruption. Les nouveaux POR du CBCB visent à intégrer en plus les aspects suivants :

1) accent stratégique à l'aide de la vision *top-down* sur les opérations ou les prestations de services les plus importantes du point de vue stratégique, qualifiées dans la circulaire de « fonctions critiques » ;

2) accent préventif à l'aide de mesures de prévention ciblées, d'un apprentissage continu et d'améliorations, afin de concevoir les fonctions critiques les plus résistantes possibles.

La gestion des risques opérationnels soutient également la résilience opérationnelle. Si la tolérance au risque est clairement définie pour les risques opérationnels et que ces derniers sont réduits en conséquence, le risque d'interruptions significatives ainsi que leurs conséquences tendent eux aussi à diminuer.

Le document mentionné du CBCB définit les objets particulièrement dignes de protection, dans le cadre de la garantie de résilience opérationnelle de l'établissement, comme étant des *critical operations*. *Operations* peut se traduire par différents termes, comme « opérations », « services » (utilisé par les autorités britanniques) ou « fonctions ». Les interprétations de ces mots en Suisse ne sont pas très éloignées les unes des autres. Le terme de « fonctions » a été choisi pour traduire *operations* pour les raisons suivantes :

- concordance avec la communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA », qui parle de « fonctions d'importance critique » ;

- concordance avec l'art. 8 al. 1 LB, où sont définies les « fonctions économiques d'importance systémique ». Celles-ci incluent notamment les opérations nationales de placement et de crédit ainsi que le trafic des paiements ;

- pas d'utilisation du terme « services » pour éviter les malentendus, car il pourrait être associé de façon limitative à des produits ou à des services à la clientèle uniquement ;

- distinction avec les « processus d'exploitation critiques » ou les « processus critiques » comme utilisés dans le BCM jusque-là ou nouvellement utilisés. De tels processus peuvent soutenir les fonctions critiques, mais ils n'en constituent que des composantes partielles.

Les « fonctions critiques » de la nouvelle circulaire incluent (Cm 14) :

a. pour tous les établissements : les activités, les processus, les services et les ressources sous-jacentes nécessaires à leur réalisation, dont l'interruption mettrait en danger la poursuite de l'établissement ou son rôle sur le marché financier et donc le bon fonctionnement des marchés financiers ; et

b. pour les banques d'importance systémique selon l'art. 8 LB : les fonctions économiques d'importance systémique selon l'art. 8 al. 1 LB.

En ce qui concerne les « processus » mentionnés au point a), il faut partir du principe que les processus nécessaires à l'exécution des fonctions critiques sont toujours des « processus critiques » au sens de la terminologie utilisée dans le BCM. À l'inverse, tous les processus critiques ne sont pas pertinents pour les fonctions critiques (Cm 8 et 14).

Les objectifs de protection visés par la résilience opérationnelle et le BCM sont différents, mais se chevauchent en partie. Comme expliqué au chapitre 4.1.7 ci-dessus, le BCM vise à garantir la réalisation des objectifs commerciaux en cas d'interruptions majeures des processus critiques (Cm 8 et 9). La garantie de la résilience opérationnelle vise à ce que l'établissement puisse poursuivre ses activités et que son rôle sur le marché financier ne soit pas affecté (Cm 14 et 16). Cela permet d'écarter les conséquences beaucoup plus graves et le nombre d'objets devant être particulièrement protégés est inférieur à celui du BCM, comme présenté dans l'illustration 1.

La protection du rôle sur le marché financier ne veut pas dire que l'attention de l'établissement doit être limitée à lui-même (Cm 14). Les objectifs de la surveillance des marchés financiers selon l'art. 4 LFINMA sont aussi pertinents du point de vue de la garantie de la résilience opérationnelle, c.-à-d. la protection des créanciers, des investisseurs et des assurés ainsi que la protection du bon fonctionnement des marchés financiers.

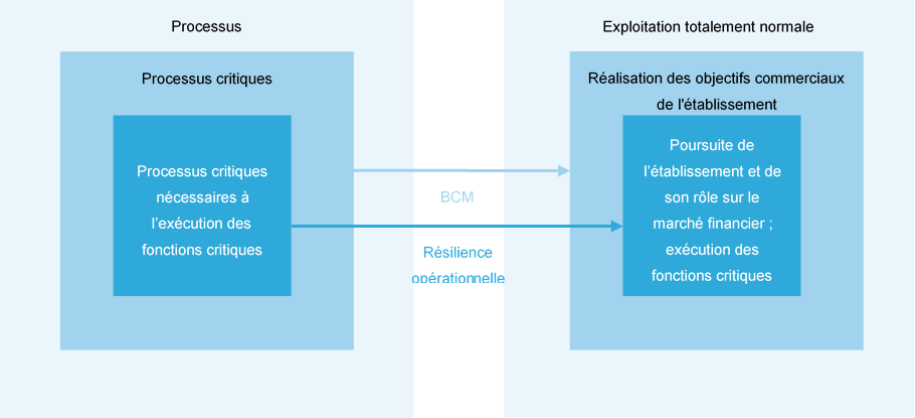

Illustration 1 : Chevauchement des objectifs de protection du BCM et de la résilience opérationnelle

Une fonction critique comprend une vue *end-to-end* ou *front-to-back* de toute la chaîne d'approvisionnement nécessaire à son exécution et des ressources correspondantes (Cm 94). Il est possible que l'exécution d'une fonction critique requière plusieurs processus critiques. Les établissements ont tendance à inclure de nombreux processus critiques (parfois des centaines) dans leur BCM. Une assimilation des processus critiques aux fonctions critiques n'est pas indiquée. Pour chaque établissement, il ne devrait exister qu'un nombre peu élevé et facile à gérer de fonctions critiques. Si les petits établissements ont défini un nombre restreint de processus critiques, il est

toutefois envisageable, dans le cadre du principe de proportionnalité, de relier en tous points les processus critiques et les fonctions critiques.

L'illustration 2 montre la manière d'utiliser certains processus à identifier (ou processus critiques), activités et services pour exécuter les fonctions critiques. Elle présente également de manière simplifiée les ressources sous-jacentes, requises à cet effet, qu'il s'agit d'identifier ainsi que les interdépendances de toutes ces composantes. Les termes « activités » et « services » ne sont pas définis de manière plus approfondie pour prendre en compte le fait qu'il existe des différences dans la terminologie utilisée par les établissements et qu'une certaine flexibilité est admise à cet égard.

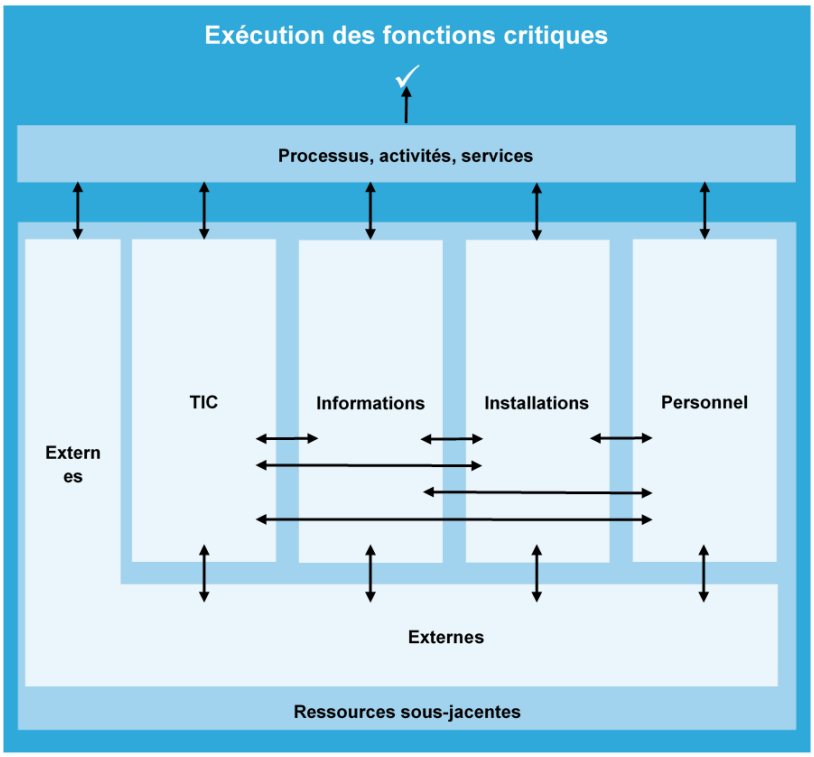

Illustration 2 : Composantes nécessaires à l'exécution des fonctions critiques

Lors de l'identification des ressources sous-jacentes nécessaires, il convient de procéder de manière granulaire et d'étendre largement le réseau afin d'obtenir une compréhension aussi transparente que possible des ressources nécessaires (Cm 94). Peuvent être des ressources potentielles :

- externes : prestataires de services, prestataires de *cloud*, commentaires pertinents des contreparties (par ex. banques centrales, chambres de compensation, autres banques, etc.), approvisionnement en électricité, bailleurs d'immeubles ou d'infrastructure, consultants) ;

- TIC : applications TIC dans les divisions, systèmes IT de base, infrastructure IT sous-jacente (par ex. centres de calcul et sites alternatifs), télécommunication ;

- informations : *inputs*, données et série de données requises pour l'exécution des fonctions critiques ;

- infrastructure : immeuble et postes de travail, équipement des postes de travail (y compris les ordinateurs portables) et organisation du télétravail), dispositif *trading desk* ;

- personnel : équipes pertinentes, différents domaines de l'établissement contribuant à exécuter la fonction critique, personnes clés, capacités spécifiques du personnel.

Il est important de comprendre les liens et les interdépendances existant tant au sein de l'établissement qu'avec les parties externes qui fournissent des informations pertinentes. Cela permet de comprendre les conséquences de diverses interruptions et de prendre des mesures afin de pouvoir continuer d'exécuter la fonction critique malgré ces interruptions.

Lors de l'identification des ressources nécessaires, des liens et des interdépendances, il est possible que différentes ressources se révèlent plus importantes que d'autres et, par conséquent, qu'elles doivent être spécialement protégées.

La notion de « tolérance aux interruptions » est introduite dans le cadre de la garantie de la résilience opérationnelle (Cm 15). Elle est définie pour chaque fonction critique et décrit dans quelle ampleur l'établissement peut tolérer l'interruption de la fonction critique. L'ampleur peut être mesurée de différentes manières : par exemple à l'aide d'une durée maximale de tolérance à l'interruption (analogue au RTO issu du BCM), une perte financière maximale tolérable découlant de l'interruption, une perturbation maximale tolérable des activités clientèle ou une perte maximale tolérable d'affaires ou de clientes et clients. L'organe responsable de la haute direction est au clair sur les conséquences des interruptions ainsi que les tolérances aux interruptions définies et les approuve (Cm 90). La capacité de fournir des fonctions critiques dans le cadre de la tolérance aux interruptions est assurée par la mise en place, si nécessaire, de mesures supplémentaires permettant de respecter la tolérance aux interruptions (Cm 89).

En cas d'interruptions des fonctions critiques, il est nécessaire de partir de scénarios « graves mais plausibles » (Cm 15). Il peut s'agir ici dans un premier temps de la perte de certaines ressources importantes, mais il convient toutefois de passer rapidement à des scénarios qui prennent en compte la perte de plusieurs ressources ou de chaînes de dépendance complètes. À

titre d'exemple, on peut supposer que l'approvisionnement externe en électricité en provenance du réseau public s'interrompt à large échelle sur une période prolongée et que les durées d'alimentation continues mises à disposition dans le cadre du BCM *(uninterruptible power supply)* ne suffisent pas. La totalité ou une grande partie des systèmes IT et de télécommunication à disposition du personnel et des clients s'interrompent alors, rendant l'exécution de nombreux processus impossible et, partant, de fonctions critiques. Pour garantir la résilience opérationnelle, il faut prendre des mesures qui garantissent l'exécution des fonctions critiques dans les limites de la tolérance aux interruptions (Cm 89).

Les tolérances aux interruptions ne doivent pas être assimilées aux RTO ou aux RPO définis dans le BCM (Cm 10), car ces derniers sont plutôt spécifiques à chaque système IT. En lieu et place, les tolérances aux interruptions des fonctions critiques doivent être sélectionnées en tenant compte de l'ensemble des ressources requises, des liens et des interdépendances. Les RTO et les RPO définis dans le BCM devraient être choisis de manière à ne pas être en contradiction avec la tolérance aux interruptions. Lorsque par ex. une tolérance aux interruptions d'un jour est choisie pour une certaine fonction critique, les RTO d'un système IT nécessaire à l'exécution de cette fonction critique ne devraient pas excéder un jour.

Il est potentiellement nécessaire de définir plusieurs tolérances aux interruptions pour chaque fonction critique, afin de couvrir ses divers aspects sous-jacents (Cm 15).

La capacité à exécuter des fonctions critiques dans les limites de la tolérance aux interruptions en cas de scénarios graves mais plausibles doit être régulièrement testée (Cm 97). Ce faisant, il est possible de choisir différentes procédures de test d'intensité et d'effectivité différentes, comme le *walk-through*, des exercices *table top*, des tests localisés ou limités à la défaillance de certaines ressources, des tests globaux (hypothèse de défaillance complète). Lors de la planification des tests, l'effectivité de ces derniers est comparée aux risques. Il faut partir du principe que certains scénarios graves mais plausibles ne peuvent pas être entièrement testés en direct, par ex. une interruption d'électricité de longue durée. Dans ces cas, il est possible d'effectuer des simulations comme les exercices *table top* ; toutefois, il est important de tenir compte des divers liens et interdépendances identifiés.

4.1.9 Principe 8 : maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique (Cm 99)

Outre une reformulation linguistique sans pertinence sur le fond, aucune modification n'a été effectuée. Les banques d'importance systémique mentionnées dans ce principe sont les banques d'importance systémique selon l'art. 8 al. 3 LB.

4.2 Circulaire FINMA 2013/3 « Activités d'audit »

La révision totale de la Circ.-FINMA 08/21 a des répercussions sur la Circ.-FINMA 13/3 « Activités d'audit » qui doivent être reproduites dans le domaine des banques et des maisons de titres. Pour les autres domaines de surveillance indirectement concernés par les adaptations dans le domaine des risques opérationnels, des adaptations analogues seront examinées séparément à moyen terme.

Ainsi, dans les activités d'audit auprès des banques et des maisons de titres, certains champs d'audit existants seront renommés, deux nouveaux champs d'audit seront créés et certaines stratégies d'audit standard seront adaptées.

Le champ d'audit « Informatique (IT) » est notamment divisé en deux champs d'audit, l'un portant sur la « gestion des risques liés à la TIC » et l'autre sur la « gestion des cyberrisques ». Cela permet de clarifier l'attribution aux principes 2 et 3 correspondants ainsi que leur délimitation mutuelle et de créer une plus grande transparence sur la couverture de la gestion des cyberrisques. Pour le champ d'audit des risques liés à la TIC, la couverture graduelle s'étend désormais sur quatre ans au lieu de six ans, d'une part en raison de la nécessité de suivre les évolutions technologiques rapides grâce à un cycle d'examen plus rapide et, d'autre part, pour des raisons conceptuelles, car le principe 2 est désormais divisé en quatre domaines et se prête donc à une couverture sur quatre ans. Les « points d'audit relatifs à l'informatique » existants sont remplacés par de nouveaux « points d'audit sur la gestion des cyberrisques ».

Le champ d'audit « Traitement des données électroniques des clients », qui se réfère à l'annexe 3 de la Circ.-FINMA 08/21, est modifié en « Gestion des risques des données critiques », conformément au nouveau principe 4, et les anciens « Points d'audit concernant le traitement des données électroniques des clients » sont révisés et renommés en conséquence.

Le champ d'audit « Exigences qualitatives concernant la gestion des risques opérationnels » est renommé « Exigences générales en matière de gestion des risques opérationnels », conformément au principe 1 de la nouvelle circulaire, sans adaptation substantielle du contenu. Aucune adaptation n'est

nécessaire pour le champ d'audit « BCM (business continuity management) ».

Pour couvrir le nouveau principe 7 relatif à la résilience opérationnelle, le nouveau champ d'audit « Résilience opérationnelle » est introduit, auquel s'applique la stratégie d'audit standard habituelle selon les Cm 87.1 à 90 de la Circ.-FINMA 13/3. En raison des différences conceptuelles avec les champs d'audit déjà existants et afin de créer la transparence sur la couverture de la résilience opérationnelle, il a été renoncé à intégrer ce thème dans un champ d'audit déjà existant.

En outre, la disposition transitoire du Cm 150 est obsolète et est supprimée.

5 Processus de réglementation

La FINMA applique un processus de réglementation transparent, prévisible et crédible, qui intègre à un stade précoce les parties impliquées et les milieux intéressés, comme les autorités et éventuellement les sciences. Une audition publique est organisée pour les modifications apportées aux ordonnances et aux circulaires (sauf en cas d'adaptations purement formelles). Les personnes concernées font un vif usage de la possibilité de prendre position dans le cadre de ces auditions. Le conseil d'administration de la FINMA en tant qu'organe compétent évalue les prises de position et expose à chaque fois dans un rapport (rapport sur les résultats) dans quelle mesure celles-ci sont mises en œuvre. Tous les documents relatifs aux auditions, y compris le rapport sur les résultats, sont publiés.[8]

5.1 Consultation préalable

Avant l'ouverture de la procédure d'audition, la FINMA procède en principe à des consultations préalables des personnes concernées et des milieux intéressés. Elle clarifie alors les faits déterminants et recueille les informations nécessaires, explique l'orientation du projet de réglementation et enregistre les appréciations correspondantes. L'échange porte sur les actions requises et les options éventuelles.

En octobre et en novembre 2021, la FINMA a procédé, dans le cadre d'un groupe de travail, à une consultation préalable d'une vingtaine de représentants de la branche. Les participants ont transmis leurs commentaires écrits portant sur le premier projet de circulaire. Par la suite, les préoccupations principales ont été discutées dans le cadre d'une conférence téléphonique. La consultation préalable portait sur les principes 1 à 4 ainsi que 6 et 7. Les

[8] Les documents relatifs aux auditions concernant les révisions d'ordonnances et de circulaires de la FINMA sont publiés sur le site Internet de la FINMA (www.finma.ch > Documentation > Auditions).

principes 5 et 8 ont été repris sans changement majeur de la Circ.-FINMA 08/21.

La majorité des passages pour lesquels les participants ont relevé un besoin d'adaptation ou de clarification ont pu être pris en compte dans le présent projet d'audition, dans la mesure où ils étaient conciliables avec les dispositions du droit supérieur et les objectifs visés par la surveillance des marchés financiers. Ainsi, des définitions terminologiques ont été révisées et des dispositions transitoires introduites pour garantir la résilience opérationnelle.

Les exigences en matière de fonds propres pour les risques opérationnels, qui ne font plus l'objet de la présente circulaire, ont été discutées séparément dans le cadre du « Groupe national de travail Bâle III final ».

5.2 Consultation des unités administratives également intéressées

Du 14 février au 8 mars 2022, la FINMA a consulté les unités administratives également intéressées.

5.3 Consultation publique

Les présentes réglementations n'ont pas une grande portée dans le sens de la loi sur la consultation du 18 mars 2005 (RS 172.061). Par conséquent, la FINMA procède à une audition conformément à l'art. 10 al. 2 de l'ordonnance relative à la loi sur la surveillance des marchés financiers du 13 décembre 2019 (RS 956.11). Le délai d'audition est de deux mois.

6 Principes de réglementation[9]

S'agissant des actions requises sur le plan réglementaire, il est fait référence au chapitre 2.

Les concrétisations de la pratique prudentielle de la FINMA exposées dans la circulaire reposent sur les normes internationales du CBCB. Les possibilités de variantes dans la définition de la réglementation étaient donc restreintes au niveau de la FINMA. En l'existence de telles variantes, elles ont été discutées dans les commentaires supra sur les différentes dispositions. À cet égard, la FINMA a privilégié les solutions qui respectent le mieux le principe de proportionnalité. Elle a tenu compte des effets sur la viabilité et la compétitivité internationale de la place financière suisse, dès lors que cela semblait pertinent.

[9] Selon l'art. 6 de l'ordonnance relative à la loi sur la surveillance des marchés financiers.

Les réglementations adoptées sont neutres sur les plans de la concurrence et de la technologie. Les règles différenciées conformément à l'art. 7 al. 2 let. c LFINMA doivent tenir compte des risques et du but visé par la réglementation (cf. également le chapitre 4.1.1 sur le principe de proportionnalité). La FINMA a respecté les normes internationales en matière de marchés financiers, pour autant qu'elles soient pertinentes, et leur mise en œuvre sur d'autres places financières importantes. Pour les détails, il est fait référence aux commentaires des différentes dispositions.

7 Analyse des effets[10]

7.1 Généralités

Les conséquences des réglementations doivent en principe déjà être présentées en détail au niveau de la loi. Les conséquences sont également présentées dans le cadre de l'édiction d'ordonnances du Conseil fédéral (en référence à l'analyse d'impact au niveau de la loi). Nous nous référons à cet égard aux lois et aux ordonnances du Conseil fédéral citées au chapitre 1.

Par rapport à la Circ.-FINMA 08/21, les exigences supplémentaires posées à la gestion des risques opérationnels et à la garantie de résilience opérationnelle visent avant tout à préciser la situation.

7.2 Conséquences de la nouvelle circulaire FINMA « Risques et résilience opérationnels – banques »

La nature et l'ampleur des conséquences de la nouvelle circulaire diffèrent selon le principe adapté. Les aspects principaux sont traités ci-après pour chacun d'entre eux.

- *Principe 1 : gestion des risques opérationnels :* la révision n'engendre pas d'adaptations fondamentales des exigences. Elle vise à remédier aux erreurs d'interprétation et aux lacunes fréquentes en lien avec les principes 1 à 3 de la Circ.-FINMA 08/21. Les nouvelles charges induites par la mise en œuvre sont estimées comme faibles à négligeables. La révision favorisera en particulier une meilleure compréhension, d'une part du rôle de la tolérance au risque dans le domaine des risques opérationnels, et d'autre part de l'importance de disposer de mesures de contrôle et d'atténuation efficaces.

- *Principe 2 : gestion des risques TIC :* le nouveau principe remplace le principe 4 « infrastructure technologique » de la Circ.-FINMA 08/21 et le

[10] Selon l'art. 7 de l'ordonnance relative à la loi sur la surveillance des marchés financiers.

précise sur la base des documents du CBCB. Il expose les bases fondamentales d'un bon fonctionnement de la TIC et reflète ainsi la pratique de surveillance déjà existante de la FINMA, qui est formulée de manière plus explicite. Pour cette raison, l'effort de mise en œuvre est estimé comme plutôt faible.

- *Principe 3 : gestion des cyberrisques :* la seule adaptation substantielle relative à la gestion des cyberrisques par rapport à la Circ.-FINMA 08/21 est l'introduction de cyberexercices fondés sur des scénarios comme l'une des possibilités de protéger les TIC et les données critiques. De plus, le projet a intégré l'annonce de cyberattaques cruciales conformément à la communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA ». Le reste de la révision vise à remédier aux erreurs d'interprétation et aux lacunes fréquentes en lien avec la Circ.-FINMA 08/21. Le recours aux cyberexercices fondés sur des scénarios ou aux autres tests cités (par ex. tests d'intrusion) est soumis – comme tous les autres chiffres marginaux – au principe de proportionnalité. Cela ne veut pas dire que tous les établissements devraient effectuer l'ensemble des tests mentionnés : pour les grands établissements complexes, les cyberexercices fondés sur des scénarios font déjà partie de la gestion appropriée des cyberrisques ; s'agissant des petits établissements, aucun exercice complexe n'est attendu de leur part compte tenu du principe de proportionnalité. De ce fait, l'effort supplémentaire de mise en œuvre est estimé comme globalement faible.

- *Principe 4 : gestion des risques des données critiques :* si le nouveau principe 4 renonce à la granularité présentée dans l'annexe 3 de la Circ.-FINMA 08/21, il élargit toutefois la définition des données devant être protégées conformément aux documents du CBCB. Celles-ci ne se limitent plus aux données clientèle électroniques, mais couvrent désormais les données considérées comme critiques en matière de confidentialité, d'intégrité ou de disponibilité. On part du principe que la majorité des établissements disposent déjà des mesures protectrices correspondantes pour leurs données critiques ; la mise en œuvre pourrait toutefois occasionner un effort supplémentaire pour certains d'entre eux.

- *Principe 6 : business continuity management (BCM) :* le principe 6 est une version actualisée, fondée sur des principes, conforme aux documents du CBCB, des « Recommandations de l'ASB en matière de Business Continuity Management (BCM) » existantes. Son contenu n'est pas fondamentalement nouveau et ne requiert aucune adaptation substantielle. L'effort induit par la mise en œuvre est estimé comme faible.

- *Principe 7 : résilience opérationnelle :* le principe 7 est nouveau et laisse anticiper des efforts supplémentaires pour sa mise en œuvre. Selon la maturité du BCM déjà existant, les efforts sont considérés comme

faibles en particulier auprès des petits établissements. Les connaissances disponibles sur les processus critiques, les BIA effectués de manière granulaire, les tests ainsi que les rapports existants sont susceptibles de fournir une grande partie des composantes requises.

La proportionnalité de la révision totale découle du fait que le respect des principes est nécessaire pour saisir, limiter et surveiller de manière appropriée les risques opérationnels (y compris les risques d'interruptions).

De plus, renoncer à la révision de la circulaire pendant une période prolongée aboutirait à des lacunes et à des insécurités juridiques considérables. En outre, il existerait un risque accru d'être jugé « non (suffisamment) *compliant* » lors des futures évaluations du CBCB, ce qui nuirait à la réputation de la place financière.

Dans ce contexte, diverses variantes ont été examinées, dont celle en particulier de la révision partielle. Celle-ci a été rejetée au vu de l'abondance des thèmes à actualiser et de leur importance.

Il a été envisagé de scinder le nouveau principe de résilience opérationnelle et de l'intégrer dans un ou plusieurs principes existants. Toutefois, cette variante n'a pas été retenue pour ne pas perdre l'accent placé sur les fonctions critiques ainsi que les aspects stratégiques et préventifs de la résilience opérationnelle. De plus, une telle dissociation distinguerait la Suisse des autres juridictions et nuirait à la réputation de la place financière. En outre, le BCM disponible jusque-là est souvent – mais pas nécessairement dans tous les établissements – trop limité[11]. Il suppose habituellement un défi « asymétrique », pour lequel seul l'établissement lui-même, une partie de l'établissement ou un nombre réduit d'établissements seraient concernés. La pandémie de coronavirus a montré que les défis « symétriques », où tous les participants du marché financiers pouvaient être affectés simultanément, étaient aussi réalistes. De tels défis symétriques sont possibles notamment comme conséquences de cyberattaques à large échelle, de coupures ou de pénuries d'électricité durables. Lors de la garantie de la résilience opérationnelle, il s'agit, en termes simplifiés, de pouvoir aussi surmonter de tels scénarios.

7.3 Conséquences sur le projet des activités d'audit

La nécessité d'adapter la Circ.-FINMA 13/3 « Activités d'audit » dans le domaine des banques et des maisons de titres en raison de la révision totale de la Circ.-FINMA 08/21 est décrite au chapitre 4.2. Les stratégies d'audit

[11] C'est le cas, entre autres, lorsque des interdépendances et les ressources nécessaires sont saisies insuffisamment, que les relations entre les DRP et les BCP ne sont pas ou insuffisamment établies ou que les tests ne tiennent compte que de pertes de ressources très ponctuelles.

qui y sont mentionnées concernent en particulier les établissements des catégories 3 à 5. Sans tenir compte des efforts initiaux pour les adaptations, on s'attend à une légère augmentation des coûts d'audit.

Le nouveau champ d'audit « Résilience opérationnelle » entraîne une augmentation du coût total de l'audit estimée à 1 % par an. La charge d'audit est considérée comme comparable à celle du BCM. Dans le BCM, les exigences doivent être vérifiées pour de nombreux processus critiques ; pour la résilience opérationnelle, très peu de fonctions critiques doivent être vérifiées, mais elles doivent l'être plus en profondeur. Pour la résilience opérationnelle, la réduction d'échelle pour les petits établissements et l'application du principe de proportionnalité sont très marquées. Plus la configuration est simple, plus l'audit nécessaire est simplifié et moins étendu.

La charge d'audit du nouveau champ d'audit « Gestion des risques liés à la TIC » est réduite à environ 60 à 80 % de l'ancien champ d'audit « Informatique (IT) » pour deux raisons : tout d'abord, en raison de la révision conceptuelle et de la concentration sur quatre domaines thématiques, avec suppression des points d'audit relatifs à l'informatique et donc suppression de l'audit détaillé de certains domaines thématiques et, ensuite, étant donné la séparation de la gestion des cyberrisques dans un champ d'audit séparé.

La réduction de la charge d'audit dans le domaine des TIC s'équilibre toutefois avec la charge d'audit pour le nouveau champ d'audit « Gestion des cyberrisques », de sorte que la division du champ d'audit « Informatique (IT) » en deux champs d'audit est globalement neutre en termes de coûts.

Là encore, sans tenir compte des efforts initiaux, les autres adaptations sont également considérées comme neutres en termes de coûts. L'accent mis sur la « gestion des risques des données critiques » est certes élargi, mais la granularité des exigences diminue en raison de la suppression de l'ancienne annexe 3. Le champ d'audit BCM ne comprenait auparavant formellement que la couverture de l'autorégulation reconnue comme standard minimal, c'est-à-dire la couverture de certains chapitres des recommandations de l'ASB pour le BCM. Toutefois, dans la pratique, l'ensemble des recommandations de l'ASB étaient déjà couvertes, ce qui est désormais le cas sous une forme condensée et actualisée avec le nouveau principe 6. L'étendue de l'audit pour les exigences qualitatives, ou nouvellement « générales » en matière de gestion des risques opérationnels, n'a pas été modifiée.

8 Suite de la procédure

À l’issue de l’audition publique, le conseil d’administration de la FINMA analysera et évaluera les prises de position reçues et exposera dans le cadre

d’un rapport sur les résultats dans quelle mesure celles-ci ont pu être mises en œuvre.

L’adoption de la nouvelle circulaire FINMA « Risques et résilience opérationnels – banques » est prévue en décembre 2022 et son entrée en vigueur le 1er janvier 2023, avec des dispositions transitoires réparties sur plus de trois ans pour le principe 7 relatif à la résilience opérationnelle (Cm 100). La révision partielle de la Circ.-FINMA 13/3 sera adoptée et entrera en vigueur en même temps.

À l’exclusion des règles régissant les exigences en matière de fonds propres, la Circ.-FINMA 08/21 sera abrogée au 1er janvier 2023. Les règles en vigueur jusqu’ici régissant les exigences en matière de fonds propres (Cm 3 à 116 Circ.-FINMA 08/21) continuent de s’appliquer momentanément durant la période transitoire entre l’entrée en vigueur de la nouvelle circulaire et l’entrée en vigueur des règles finales de Bâle III (vraisemblablement le 1er janvier 2024 ; cf. chapitre 2 supra), puis seront également abrogées. Il est fait référence à cet égard aux dispositions transitoires de la nouvelle circulaire (Cm 101).