Circulaire 22xx/xx
Risques et résilience opérationnels – banques

Gestion des risques opérationnels et garantie de la résilience opérationnelle

Référence :	Circ.-FINMA 22/xx « Risques et résilience opérationnels – banques »
Date :	...
Entrée en vigueur :	1er janvier 2023
Concordance :	remplace la Circ.-FINMA 08/21 « Risques opérationnels – banques » du 20 novembre 2008
Bases légales :	LFINMA, art. 7 al. 1 let. b et 29 al. 1 LB art. 3 al. 2 let. a et 3f OB art. 12 LEFin art. 9 OEFin art. 12 et 68
Annexe 1:	Graphiques explicatifs concernant la résilience opérationnelle

Destinataires																											
LB			**LSA**			**LEFin**						**LIMF**						**LPCC**						**LBA**		**Autres**	
Banques	Groupes et congl. financiers	Autres intermédiaires	Assureurs	Groupes et congl. d'assur.	Intermédiaires d'assur.	Gestionnaires de fortune	Trustees	Gestionnaires de fortune coll.	Directions de fonds	Maisons de titres tenant des comptes	Maisons de titres ne tenant pas de comptes	Plates-formes de négociation	Contreparties centrales	Dépositaires centraux	Référentiels centraux	Systèmes de paiement	Participants	SICAV	Sociétés en comm. de PCC	SICAF	Banques dépositaires	Représentants de PCC étr.	Autres intermédiaires	OAR	Entités surveillées par OAR	Sociétés d'audit	Agences de notation
X	X									X	X																

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

Table des matières

I. Objet et champ d'application

La présente circulaire se réfère aux prescriptions en matière de séparation des fonctions, de gestion des risques et de contrôle interne de l'ordonnance sur les banques (art. 12 OB ; RS 952.02) et de l'ordonnance sur les établissements financiers (art. 12 et 68 OEFin ; RS 954.11) et concrétise la pratique prudentielle correspondante. Ses principes tiennent compte des principes du Comité de Bâle pour une gestion irréprochable des risques opérationnels[1] et de la résilience opérationnelle[2]. 1

La présente circulaire s'adresse aux banques selon l'art. 1*a* de la loi sur les banques (LB ; RS 952.0), aux personnes selon l'art. 1*b* LB, aux maisons de titres selon les art. 2 al. 1 let. e et 41 de la loi sur les établissements financiers (LEFin ; RS 954.1) ainsi qu'aux groupes financiers et aux conglomérats financiers selon l'art. 3*c* LB et l'art. 49 LEFin. Par « établissements », on entend ci-après les banques, les maisons de titres, les groupes et conglomérats financiers . 2

II. Définitions

Les *risques opérationnels* sont définis comme étant le risque de perte lié àl'inadéquation ou à la défaillance de procédures internes, aux personnes ou aux systèmes ou encore à des facteurs externes. Sont compris les risques juridiques, mais non les risques stratégiques et les risques de réputation. 3

Les *risques inhérents* sont les risques opérationnels auxquels est exposé l'établissement en raison de ses produits, de ses activités, de ses procédures et de ses systèmes, sans prise en compte des mesures de contrôle et d'atténuation. 4

Les *risques résiduels* sont les risques opérationnels auxquels est exposé l'établissement après prise en compte des mesures de contrôle et d'atténuation. 5

Par *technologie de l'information et de la communication (TIC)*, on entend la structure physique et logique (électronique) des systèmes IT et de communication, les différentes composantes matérielles et logicielles, les réseaux, les données et les environnements d'exploitation. 6

Les *données critiques* sont des données qu'un établissement considère comme importantes pour le succès et la durabilité de ses services, ou des données qui doivent être conservées à des fins réglementaires. Les données peuvent être critiques tant en ce qui concerne la confidentialité, l'intégrité que la disponibilité. Les données critiques du point de vue de la confidentialité (données confidentielles) sont celles qui doivent être particulièrement protégées de la publication non autorisée (par ex. données personnelles, données de la clientèle, secrets professionnels). 7

Les *processus critiques* sont des processus dont l'interruption est susceptible d'entraver substantiellement la réalisation des objectifs commerciaux de l'établissement. Ils prennent en compte les conséquences financières, opérationnelles, juridiques et de réputation. 8

[1] CBCB, « Principles for Operational Resilience » ; https://www.bis.org/bcbs/publ/d516.pdf.

[2] CBCB « Revisions to the Principles for the Sound Management of Operational Risk » ; https://www.bis.org/bcbs/publ/d515.htm.

Le *business continuity management* (BCM) désigne l'approche prévue à l'échelle de l'établissement pour rétablir l'exploitation des processus critiques en cas d'interruption majeure. Le BCM traite donc, entre autres, les processus critiques qui sont nécessaires à l'exécution des fonctions critiques au sens du Cm 14 et à la garantie de la résilience opérationnelle au sens du Cm 16. La *stratégie BCM* définit la procédure fondamentale de l'établissement en matière de BCM. Elle couvre l'organisation et la gouvernance pertinentes pour le BCM, la définition des tâches, les responsabilités et les compétences ainsi que le cadre de conception des éléments du BCM mentionné dans le principe 6. 9

Le *recovery time objective* (RTO) est le délai nécessaire jusqu'au rétablissement d'une application, d'un système et/ou d'un processus. Le *recovery point objective* (RPO) est la durée maximale acceptable d'une perte de données. 10

Le *business continuity plan* (BCP) est un plan qui définit les procédures, les options de remplacement et les ressources de remplacement nécessaires (les processus de rétablissement) pour garantir la continuité et le rétablissement des processus critiques. 11

Le *disaster recovery plan* (DRP) définit les processus de rétablissement qui permettent d'atteindre les objectifs de rétablissement en cas de défaillance majeure ou de destruction de l'infrastructure technologique (par ex. matériel informatique *(hardware)*, réseaux, site primaire ou de production, centres de calcul), en tenant compte de l'éventuelle défaillance de personnes clés. 12

Les *situations de crise* sont des situations qui ne peuvent pas être maîtrisées à l'aide de mesures ou de compétences décisionnelles ordinaires. 13

Les *fonctions critiques* comprennent : 14

a. 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. les fonctions d'importance systémique selon l'art. 8 LB.

La *tolérance aux interruptions* est l'ampleur (par ex. durée ou dommages attendus) de l'interruption d'une fonction critique que l'établissement est disposé à accepter en tenant compte de scénarios graves mais plausibles. Une tolérance aux interruptions doit être définie pour chaque fonction critique. 15

La *résilience opérationnelle* désigne la capacité de l'établissement à pouvoir rétablir ses fonctions critiques en cas d'interruptions dans les limites de la tolérance aux interruptions, c.-à-d. la capacité de l'établissement à identifier les menaces et les défaillances éventuelles, à s'en protéger et à y réagir, à rétablir la marche ordinaire des affaires en cas d'interruptions et à en tirer des enseignements pour minimiser les conséquences sur l'exécution des fonctions critiques. 16

III. Principe de proportionnalité

Les principes présentés ci-après s'appliquent fondamentalement à l'ensemble des destinataires de cette circulaire. Ils doivent cependant être mis en œuvre au cas par cas en 17

fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement.

Les banques et les maisons de titres des catégories FINMA 4 et 5 sont exemptées du respect des Cm 30 et 31, 33 et 34, 37, 43, 49, 61 et 62, 64 à 66, 68, 79, 84 et 85, 88, 90 et 91 ainsi que 97 à 99. La FINMA ordonne des allègements ou des renforcements au cas par cas. 18

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 sont en plus exemptés du respect des exigences des Cm 60, 63, 67, 69 et 70 ainsi que 92 à 96. 19

IV. Principes

A. Principe 1 : exigences générales en matière de gestion des risques opérationnels

Les exigences en matière de structures organisationnelles, de politique de risque et de grandes lignes de la gestion des risques à l'échelle de l'établissement conformément à la circulaire FINMA 2017/1 « Gouvernance d'entreprise – banques » s'appliquent aussi à la gestion des risques opérationnels. 20

La direction met en œuvre et documente une gestion des risques opérationnels qui traite l'ensemble des risques opérationnels pertinents pour l'établissement, dont en particulier les risques abordés à titre complémentaire dans les principes 2 à 5. 21

L'organe responsable de la haute direction selon le chapitre IV de la Circ.-FINMA 17/1 approuve et surveille régulièrement la gestion des risques opérationnels ; il décide au moins une fois par année de la tolérance au risque en matière de risques opérationnels compte tenu des objectifs stratégiques et financiers de l'établissement. Ce faisant, il tient compte des résultats issus des évaluations de risques et de contrôle selon le Cm 27. Soit il accepte le degré d'exposition aux risques opérationnels de l'établissement, soit il décide d'une adaptation de la tolérance au risque et des modifications stratégiques nécessaires[3]. 22

Pour le pilotage et le contrôle des risques inhérents considérés comme principaux, la direction doit, en fonction de la situation, définir et mettre en œuvre des mesures complémentaires spécifiques au risque ou renforcer les mesures existantes. 23

Si nécessaire, la FINMA définit, 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. 24

Les risques opérationnels doivent être catégorisés de façon uniforme à l'échelle de l'établissement et répertoriés dans un inventaire. Cette catégorisation uniforme peut être effectuée en s'appuyant sur la catégorisation des types d'événements utilisée dans le cadre du calcul des fonds propres minimaux pour les risques opérationnels ou au moyen d'une taxonomie interne. Elle doit être appliquée systématiquement dans tous les domaines de l'établissement et dans toutes les composantes de la gestion des risques opérationnels. 25

[3] Par exemple un changement de modèle d'affaires.

Des facteurs internes[4] et externes[5] sont pris en compte dans l'identification des risques opérationnels. Les risques opérationnels identifiés sont évalués tant du point de vue des risques inhérents que des risques résiduels. 26

L'identification et l'évaluation des risques opérationnels s'appuient au moins sur les résultats d'audit[6] et les évaluations des risques et des contrôles à effectuer régulièrement. Les évaluations des risques et des contrôles tiennent compte des risques inhérents, de l'efficacité des mesures de contrôle et d'atténuation existantes ainsi que des risques résiduels. 27

Pour évaluer les mesures de contrôle et d'atténuation existantes, il est en particulier procédé à un examen régulier indépendant de l'efficacité des contrôles clés (*design effectiveness* et *operating effectiveness testing*). Les contrôles clés sont les mesures de contrôle et d'atténuation qui diminuent les risques inhérents considérés comme principaux. La séparation des tâches, des responsabilités et des compétences pour garantir l'indépendance et prévenir les conflits d'intérêts fait l'objet d'évaluations régulières. 28

Des évaluations des risques et des contrôles doivent être effectuées en cas de changements importants dans les produits, les activités, les procédures et les systèmes. Celles-ci prennent en compte les risques opérationnels découlant du processus de changement ainsi que les risques opérationnels de l'état cible. La tolérance au risque est adaptée si besoin. 29

En fonction de la nature, de l'ampleur, de la complexité et de la teneur en risque des produits, activités, procédures et systèmes spécifiques à l'établissement, il s'agit d'appliquer les instruments et méthodes supplémentaires suivants : 30

a. la collecte et l'analyse systématiques des données de pertes internes et des incidents externes pertinents liés à des risques opérationnels ;

b. les indicateurs de risque et de contrôle pour la surveillance des risques opérationnels et l'identification rapide des hausses pertinentes selon le degré d'exposition de l'établissement aux risques ;

c. les analyses de scénario et/ou l'estimation du potentiel de perte compte tenu/vis-à-vis des fonds propres minimaux pour les risques opérationnels ;

d. les analyses comparatives *(read across)*, comme les analyses de pertinence des résultats d'audit pour d'autres domaines de l'établissement ou des comparaisons croisées entre les résultats issus des évaluations des risques et des contrôles de différents domaines.

La tolérance au risque pour les risques opérationnels tient compte de la tolérance en lien tant avec les risques inhérents qu'avec les risques opérationnels résiduels. Elle fait l'objet d'une surveillance au moyen d'indicateurs de risque et de contrôle. 31

[4] Sont considérés comme facteurs internes par ex. les changements apportés aux produits, aux activités, aux processus et aux systèmes, les résultats d'audit et les pertes internes issues des risques opérationnels.

[5] Sont considérés comme facteurs externes par ex. les événements de perte reconnus d'autres établissements, les changements sur le plan de la sécurité (par ex. en raison d'influences environnementales ou du terrorisme) ou les changements en matière d'exigences réglementaires.

[6] Les résultats d'audit comprennent les résultats des audits effectués par la révision interne et la société d'audit externe, si disponibles, ainsi que les résultats d'examens effectués par ex. par les domaines commerciaux et organisationnels, le contrôle des risques, la fonction de *compliance* ou les autorités de surveillance.

Le contrôle des risques rend compte à l'organe responsable de la haute direction et à la direction selon les Cm 75 et 76 de la Circ.-FINMA 17/1 au moins des risques opérationnels auxquels l'établissement est exposé, de la comparaison avec la tolérance au risque fixée ainsi que des détails concernant les pertes internes importantes et les résultats d'audit importants selon la note de fin de page 6. 32

Le compte rendu interne au sens du Cm 32 contient à titre complémentaire les informations suivantes : 33

- les facteurs externes pertinents selon la note de fin de page 5,
- l'efficacité des contrôles clés selon le Cm 28,
- les risques opérationnels émergents,
- les résultats découlant de l'application des instruments et des méthodes supplémentaires selon le Cm 30.

De plus, l'établissement rend compte régulièrement des risques opérationnels sur le plan des domaines commerciaux et organisationnels exposés à des risques opérationnels pertinents ou principaux. 34

B. Principe 2 : gestion des risques TIC

a) Stratégie TIC et gouvernance

L'organe responsable de la haute direction définit une stratégie TIC, qui est coordonnée avec la stratégie commerciale. La direction met en œuvre et documente la gestion des risques TIC, qui est étroitement coordonnée avec la stratégie TIC et la tolérance au risque correspondante. 35

La gestion des risques TIC garantit que les risques TIC en lien avec les processus critiques de l'établissement sont identifiés, évalués, limités et surveillés. De plus, elle contribue à l'efficacité du système de contrôle interne. 36

Lorsque la gestion des risques TIC est établie, il faut tenir compte des bonnes pratiques et des normes pertinentes reconnues à l'échelle internationale, de même que des nouvelles évolutions technologiques. 37

En fonction de la tolérance au risque fixée, la gestion des risques TIC doit comporter des mesures destinées à renforcer la prise de conscience par les collaborateurs de leur fonction et de leur responsabilité concernant la réduction des risques TIC[7]. 38

L'organe responsable de la haute direction surveille régulièrement l'efficacité de la gestion des risques TIC. La direction évalue régulièrement l'organisation et la mise en œuvre de la gestion des risques TIC. 39

La gestion des risques TIC implique un compte rendu régulier à la direction sur l'évolution des risques, des contrôles et des incidents TIC. 40

La direction s'assure que des procédures, des processus, des contrôles, des tâches, des fonctions et des responsabilités soient implémentés et documentés tant pour la gestion 41

[7] Cela inclut notamment la sélection rigoureuse et la qualification du personnel pour ses tâches ainsi que sa formation continue permanente dans le cadre de ses activités.

des changements *(change management)* que pour l'exploitation TIC *(run, maintenance)*. Ceux-ci sont dotés de ressources qualifiées et appropriées.

b) Gestion des changements *(change management)*

La gestion des changements définit des procédures, des processus et des contrôles pour toutes les phases de développement et d'acquisition de TIC, et prend en compte dans chaque phase les conséquences sur les risques TIC et les changements qui en découlent. Ce faisant, l'accent est mis notamment sur les objectifs liés à la confidentialité, l'intégrité et la disponibilité. 42

Il faut garantir la séparation entre, d'une part, les environnements TIC de développement ou de test et, d'autre part, les environnements de production TIC. Cela comprend également une attribution claire de tâches, de fonctions et de responsabilités ainsi qu'une réglementation des autorisations d'accès afférentes. 43

Lors du développement et de l'acquisition de TIC, les exigences fonctionnelles et non fonctionnelles (par ex. en ce qui concerne l'architecture, les exigences à l'égard de la sécurité de l'information) sont clairement définies et approuvées, puis testées et validées selon leur criticité. 44

c) Exploitation TIC *(run, maintenance)*

L'établissement dresse un inventaire des composantes TIC. L'inventaire inclut les composantes matérielles et logicielles ainsi que les lieux de sauvegarde des données critiques. Il tient compte des dépendances internes ainsi que des interfaces avec les prestataires externes importants. 45

L'inventaire est disponible rapidement et est régulièrement vérifié et mis à jour. 46

L'établissement dispose de procédures, de processus et de contrôles qui garantissent la confidentialité, l'intégrité et la disponibilité de l'environnement de production TIC en tenant compte du besoin de protection. 47

L'établissement garantit des transitions consistantes entre la gestion opérationnelle TIC et les procédures BCM et DRP. Il met en œuvre des procédures de sauvegarde et de restauration appropriées, qui sont régulièrement testées et validées. 48

L'établissement dispose de procédures, de processus et de contrôles qui garantissent une gestion orientée vers le risque des TIC dont la fin de l'exploitation approche ou dont la mise hors service prévue a été dépassée. 49

d) Gestion des incidents *(incident management)*

L'établissement dispose de procédures, de processus et de contrôles visant à traiter les incidents TIC importants, y compris ceux qui sont dus à des dépendances vis-à-vis de prestataires externes importants ou à des externalisations au sein d'un groupe. Il y a lieu de tenir compte de l'ensemble du cycle de vie des incidents TIC importants et de définir des tâches, des rôles et des responsabilités pour traiter ces incidents. 50

Le traitement des incidents TIC importants doit être coordonné et rattaché aux processus BCM et DRP. 51

Les établissements renseignent sans délai la FINMA sur les incidents TIC qu'ils considèrent comme des perturbations importantespour l'exécution de leurs processus critiques et qui sont susceptibles de l'intéresser (cf. art. 29 al. 2 LFINMA). 52

C. Principe 3 : gestion des cyberrisques

La direction garantit la gestion des cyberrisques, qui englobe l'identification, l'évaluation, la limitation et la surveillance en tenant compte de la tolérance au risque et en conformité avec la stratégie liée aux cyberrisques. La gestion des cyberrisques est inclue dans la gestion des risques opérationnels et documentée de façon compréhensible. 53

La gestion des cyberrisques contient au moins un rapport annuel à la direction sur l'évolution des cyberrisques, l'efficacité des contrôles clés et les incidents internes et externes importants. 54

De plus, la gestion des cyberrisques définit des tâches, des rôles et des responsabilités clairs. Elle doit couvrir au moins les aspects suivants selon les meilleures pratiques et normes internationalement reconnues et garantir, développer et améliorer continuellement leur mise en œuvre effective au moyen de procédures, de processus et de contrôles appropriés : 55

a. identification des menaces potentielles liées aux cyberattaques[8] spécifiques à l'établissement et évaluation des conséquences possibles liées à l'exploitation des faiblesses relatives aux composantes TIC répertoriées (selon Cm 45 et 46) ;

b. protection des processus critiques contre les cyberattaques par l'implémentation de mesures de protection appropriées, en particulier en ce qui concerne la confidentialité, l'intégrité et la disponibilité des données critiques et des systèmes IT ;

c. détection et enregistrement rapides des cyberattaques sur la base d'un processus de surveillance systématique et complet des TIC ;

d. réaction aux faiblesses et aux cyberattaques identifiées par le développement et l'implémentation de processus appropriés, permettant de prendre rapidement des mesures d'atténuation et de suppression ; et

e. garantie d'un rétablissement rapide de la marche ordinaire des affaires après des cyberattaques, grâce à des mesures appropriées.

La gestion des cyberrisques doit garantir qu'une cyberattaque, qu'elle ait atteint son but entièrement ou partiellement, soit analysée selon son importance pour les systèmes et processus critiques (y compris les fonctions et services externalisés) et que l'obligation d'annoncer selon l'art. 29 al. 2 LFINMA soit respectée. Après une première évaluation et une information préalable à la FINMA dans les 24 heures, l'annonce doit être transmise dans les 72 heures au service compétent de la FINMA, conformément au cahier des charges de la plate-forme de saisie (champs obligatoires). Une fois que le cas a été traité par l'établissement, un rapport conclusif sur les causes conforme au degré de gravité doit être remis. 56

[8] Attaques en provenance du réseau interne, d'Internet et de réseaux analogues contre la confidentialité, l'intégrité et la disponibilité des TIC ainsi que les données critiques.

De plus, l'établissement doit mettre en œuvre des mesures destinées à renforcer la prise de conscience par les collaborateurs de leur fonction et de leur responsabilité concernant la réduction des cyberrisques. 57

La direction ordonne régulièrement des analyses de vulnérabilité[9], des tests d'intrusion[10] et des cyberexercices[11] fondés sur des scénarios reposant sur les menaces potentielles spécifiques à l'établissement. Ces derniers doivent être effectués en fonction du risque et par du personnel qualifié qui dispose de ressources adéquates. Les cyberexercices doivent comprendre au moins les systèmes IT qui sont nécessaires à l'exécution des processus critiques, qui contiennent des données critiques ou qui sont accessibles sur Internet. 58

D. Principe 4 : gestion des risques des données critiques

La direction met en œuvre et documente la gestion des risques des données critiques, qui garantit l'identification, l'évaluation, la limitation et la surveillance de ces risques. Cela est effectué en étroite coordination avec une stratégie systématique et complète en matière de données, avec la gestion des risques opérationnels, des risques TIC et des cyber-risques et avec la tolérance au risque correspondante. 59

La direction définit des processus, des procédures et des contrôles adéquats ainsi que des tâches, des rôles et des responsabilités clairs relatifs au traitement des données critiques identifiées par l'établissement. Par ailleurs, la direction mandate une unité indépendante à titre de fonction de contrôle pour créer et maintenir les conditions-cadres permettant de garantir la confidentialité, l'intégrité et la disponibilité des données critiques. 60

L'établissement identifie ses données critiques de manière systématique et exhaustive, les catégorise sur la base du degré de confidentialité ou de criticité et définit des responsabilités claires en matière de données. 61

Les données critiques définies par l'établissement sont gérées tout au long de leur cycle de vie. 62

Dans ce cadre, des processus, des procédures et des contrôles appropriés garantissent en particulier le respect de la confidentialité, de l'intégrité et de la disponibilité lors de l'administration des données critiques. 63

Pendant le développement, le changement et la migration des TIC, l'accès et l'utilisation des données critiques par des personnes non autorisées doivent être protégés. Cela s'applique également aux données authentiques dans les environnements de test. 64

La TIC physique et logique, qui sauvegarde ou traite les données critiques, est à protéger en particulier. L'accès à ces données doit être réglementé systématiquement et surveillé en permanence. 65

[9] Analyse visant à identifier les faiblesses actuelles des logiciels ainsi que les failles de sécurité de l'infrastructure IT par rapport aux cyberattaques.

[10] Évaluation ciblée et exploitation des faiblesses des logiciels et des failles de sécurité des TIC.

[11] En tenant compte du Cm 17, ils pourraient par ex. inclure des exercices *table-top*, *red teaming*, etc.

L'accès aux données critiques et aux fonctions liées au traitement de ces données est limité aux personnes qui en ont besoin pour accomplir leurs tâches[12]. À cet égard, l'établissement doit disposer d'un système d'autorisation fondé sur les rôles et les fonctions, dont les droits d'accès doivent être régulièrement vérifiés. 66

Lorsque les données critiques sont stockées hors de Suisse[13] ou qu'elles sont accessibles depuis l'étranger, les risques accrus qui en résultent doivent être limités de manière appropriée et les données particulièrement protégées. 67

Tant les personnes internes qu'externes qui peuvent accéder aux données critiques ou les modifier doivent être soigneusement sélectionnées. Ces personnes doivent être surveillées à l'aide des mesures appropriées[14] et formées régulièrement sur le traitement de ces données. Des exigences accrues en matière de sécurité s'appliquent aux personnes bénéficiant de privilèges accrus[15]. Il convient en outre de tenir une liste de ces personnes et la mettre continuellement à jour. 68

Les incidents qui entravent de manière importante la confidentialité, l'intégrité ou la disponibilité des données critiques doivent être annoncés immédiatement à la FINMA (art. 29 al. 2 LFINMA). 69

Une grande importance doit être accordée à l'examen de diligence *(due diligence)* lors du choix des prestataires qui peuvent accéder aux données critiques ou les gérer. Il faut définir des critères clairs pour évaluer la manière dont les prestataires gèrent les données critiques et de les examiner avant de signer des contrats. Les prestataires doivent être soumis à une surveillance et à un contrôle périodiques orientés sur le risque dans le cadre du système de contrôle interne de l'établissement à l'origine de l'externalisation. 70

E. Principe 5 : gestion des risques liés aux activités de service transfrontières

Quand des établissements ou leurs filiales fournissent des services ou distribuent des produits financiers dans le cadre d'opérations transfrontières, les risques résultant d'une application des législations étrangères (droit fiscal, droit pénal, législation en matière de blanchiment d'argent, etc.) doivent également être identifiés, limités et contrôlés de façon appropriée. En tant qu'autorité de surveillance, la FINMA s'attend en particulier à ce que les banques respectent le droit étranger de la surveillance. 71

Les établissements soumettent leurs activités de services transfrontières ainsi que la distribution transfrontière de produits financiers à une analyse approfondie des conditions-cadres juridiques et des risques correspondants. Sur la base de cette analyse, les établissements prennent les mesures stratégiques et organisationnelles nécessaires à l'élimination et à la minimisation des risques et les adaptent au fur et à mesure à l'évolution de la situation. Ils possèdent notamment les connaissances spécialisées requises spécifiques aux pays, définissent des modèles de prestations spécifiques aux pays desservis, forment 72

[12] Par ex. principe du *need to know*.

[13] Par ex. à l'aide de solutions de *cloud* ou de *hosting*.

[14] Par ex. évaluation des fichiers journaux, principe des quatre yeux, etc.

[15] Par ex. les personnes qui bénéficient de droits d'administration, les utilisatrices et utilisateurs qui disposent d'un accès fonctionnel à une grande quantité de données critiques, etc.

le personnel et garantissent le respect des prescriptions grâce à des mesures organisationnelles, des directives et des modèles de rémunération et de sanction correspondants.

Les risques générés par les gérants de fortune indépendants, les intermédiaires et autres prestataires doivent également être pris en compte. En conséquence, ces partenaires doivent être choisis et instruits avec soin. 73

Ce principe s'applique également aux cas dans lesquels une filiale, une succursale ou une entité similaire d'un établissement financier suisse domiciliée à l'étranger offre des services transfrontières à des clients. 74

F. Principe 6 : *business continuity management* (BCM)

L'organe responsable de la haute direction approuve à intervalles réguliers la stratégie BCM et surveille son respect. La mise en œuvre de la stratégie incombe à la direction. 75

Chaque domaine commercial ou organisationnel pertinent doit identifier ses processus critiques et les ressources correspondantes nécessaires[16] dans le cadre de la *business impact analysis* (BIA). 76

S'agissant des processus critiques, l'établissement définit le RTO et le RPO conformément au Cm 10. Ceux-ci sont coordonnés avec les fournisseurs de prestations[17] requis à cet effet et leur respect est régi par des *service level agreements* ou des contrats, ou garantis par d'autres procédures et contrôles appropriés. 77

L'établissement définit au moins un BCP selon le Cm 11, qui décrit aussi les processus de décision ainsi que les événements déclencheurs du plan et tient compte de la perte des ressources selon le Cm 76. L'acceptation des risques résiduels est documentée de manière adéquate. 78

La BIA et le BCP sont établis et documentés de manière cohérente selon une directive applicable à l'échelle de l'établissement. Ils doivent être vérifiés chaque année ainsi qu'en cas de changements majeurs dans l'activité (réorganisations, création d'un nouveau champ d'activité, etc.). 79

L'établissement définit un DRP en tant que partie intégrante du BCP. Lorsque des parties de l'infrastructure technologie sont externalisées, le DRP renseigne sur les dépendances externes et les réglementations contractuelles ainsi que les solutions alternatives. Le DRP est revu en cas de changements majeurs, mais au moins une fois par année. 80

Dans les situations de crise, un état-major de crise est chargé de gérer la crise jusqu'au rétablissement de l'ordre légal. Les événements déclencheurs d'une crise, les responsabilités et les compétences de l'état-major de crise doivent être réglés au préalable, et l'organisation de crise doit être axée sur l'activité commerciale et la structure géographique de l'établissement. L'accessibilité des responsables en situation de crise doit être garantie. 81

L'établissement définit une stratégie de communication interne et externe en situation de crise. 82

[16] Personnel, infrastructure (par ex. immeubles, infrastructure des postes de travail), systèmes IT ou infrastructure IT (y compris systèmes de communication), dépendances vis-à-vis d'autres domaines de l'établissement et de tiers, par ex. prestataires ou fournisseurs externes (externalisation), banques centrales ou chambres de compensation.

[17] Par ex. avec le département IT, d'autres domaines de l'établissement ou des externes.

La mise en œuvre du BCP et du DRP ainsi que le bon fonctionnement de l'organisation de crise sont régulièrement soumis à des tests. À cet effet, l'établissement met en œuvre une planification de test systématique, qui garantit la couverture régulière. Il est possible de choisir plusieurs manières de procéder au test avec des degrés d'intensité et d'efficacité variables. 83

Les principales mesures au sens du BCP et du DRP ainsi que l'organisation de crise sont testées au moins une fois par année. 84

Les parties prenantes, y compris celles issues des fonctions IT et des fonctions spécialisées, participent aux tests pour se familiariser aux processus de rétablissement. 85

Les tests comprennent différents scénarios graves mais plausibles, et prennent en compte les dépendances en matière de rétablissement, y compris celles qui existent à l'égard de tiers internes ou externes. 86

Des comptes rendus réguliers informent l'organe responsable de la haute direction et la direction des activités de test et de vérification effectuées ainsi que de leurs résultats. Ils présentent clairement les priorités adoptées (par ex. priorisation des processus critiques requis pour l'exécution des fonctions critiques selon le Cm 14) et les lacunes identifiées dans la couverture d'autres processus critiques. 87

Les collaborateurs ainsi que les membres de l'organisation de crise sont suffisamment formés au sujet de leurs tâches, de leurs responsabilités et de leurs compétences qui découlent des diverses activités BCM. Cela s'applique aussi bien lors de l'entrée en fonction de nouveaux membres du personnel qu'en ce qui concerne les formations régulières de rafraîchissement. 88

G. Principe 7 : résilience opérationnelle

L'établissement identifie ses fonctions critiques et leurs tolérances aux interruptions, et prend des mesures pour garantir la résilience opérationnelle en tenant compte de scénarios graves, mais plausibles. L'organe responsable de la haute direction approuve et surveille régulièrement la procédure visant à garantir la résilience opérationnelle. 89

Les fonctions critiques et leurs tolérances aux interruptions au sens du Cm 14 doivent être approuvées par l'organe responsable de la haute direction au moins une fois par année. 90

L'établissement coordonne les composantes pertinentes d'une gestion des risques globale, comme la gestion des risques opérationnels, le *business continuity management*, la gestion des externalisations (*outsourcing* ; cf. circulaire FINMA 2018/3 « Outsourcing »), et le plan d'urgence (principe 8), pour qu'elles contribuent à renforcer la résilience opérationnelle de l'établissement. Cela inclut un échange approprié des informations pertinentes entre ces différents domaines. 91

La direction et l'organe responsable de la haute direction doivent recevoir régulièrement des rapports sur la résilience opérationnelle ainsi qu'en cas de faiblesses de contrôle importantes ou d'incidents qui menacent la résilience opérationnelle. 92

Les menaces internes et externes des fonctions critiques ainsi que l'exploitation correspondante des vulnérabilités sont identifiées et évaluées. Les risques opérationnels en résultant sont identifiés, évalués, limités et surveillés dans le cadre de la gestion des risques opérationnels. 93

L'établissement constitue un inventaire de ses fonctions critiques, qui doit être examiné et mis à jour au moins une fois par année. Cet inventaire comporte les tolérances aux interruptions des fonctions critiques ainsi que les connexions et les dépendances entre les processus critiques nécessaires et leurs ressources[18] pour exécuter les fonctions critiques. 94

Les risques opérationnels et les contrôles clés sont documentés pour les fonctions critiques. 95

Les fonctions critiques et les processus critiques et ressources nécessaires à cet effet sont couverts par les BCP selon le principe 6. 96

La capacité à exécuter des fonctions critiques dans les limites de leurs tolérances aux interruptions en cas de scénarios graves mais plausibles est régulièrement testée. Y compris sont des scénarios qui se distinguent des interruptions brèves et plutôt limitées en se démarquant par des interruptions de longue durée (par ex. plusieurs mois) et la défaillance de ressources fondamentales[19]. 97

S'agissant des banques d'importance systémique, le BCP, le DRP et l'organisation en cas de crise selon le principe 6, pertinents pour la poursuite des fonctions critiques selon le Cm 14, doivent être coordonnés avec leur plan d'urgence selon le principe 8. 98

H. Principe 8 : maintien des prestations critiques lors de la liquidation et de l'assainissement des banques d'importance systémique

Dans le cadre de leur plan d'urgence, les banques d'importance systémique prennent les mesures requises pour que leurs fonctions d'importance systémique puissent être poursuivies sans interruption (art. 9 al. 2 let. d LB en rel. avec les art. 60 ss OB). Elles identifient les requis pour la poursuite des fonctions d'importance systémique en cas de liquidation, d'assainissement ou de restructuration (« prestations critiques ») et prennent les mesures nécessaires à leur poursuite. Elles tiennent compte à cet égard des prescriptions des organismes édictant les standards internationaux. 99

V. Dispositions transitoires

A. À propos du principe 7 « Résilience opérationnelle »

L'identification des fonctions critiques et la définition des tolérances aux interruptions doivent être effectuées dans un délai transitoire d'une année à compter de l'entrée en vigueur. Un délai transitoire de deux ans à partir de l'entrée en vigueur est accordé pour effectuer l'inventaire des fonctions critiques et les premiers tests de chaque fonction critique. La garantie de la résilience opérationnelle est attendue dans un délai transitoire de trois ans à compter de l'entrée en vigueur. 100

B. À propos des exigences de fonds propres

Les exigences de fonds propres pour les risques opérationnels au sens des art. 89 ss OFR s'appuient sur les Cm 3 à 116 de la circulaire FINMA 2008/21 « Risques opérationnels – banques » jusqu'à l'entrée en vigueur le 1er juillet 2024 de l'OFR révisée dans le cadre du 101

[18] Y compris les composantes de l'inventaire pertinentes pour les fonctions critiques selon le Cm 45.

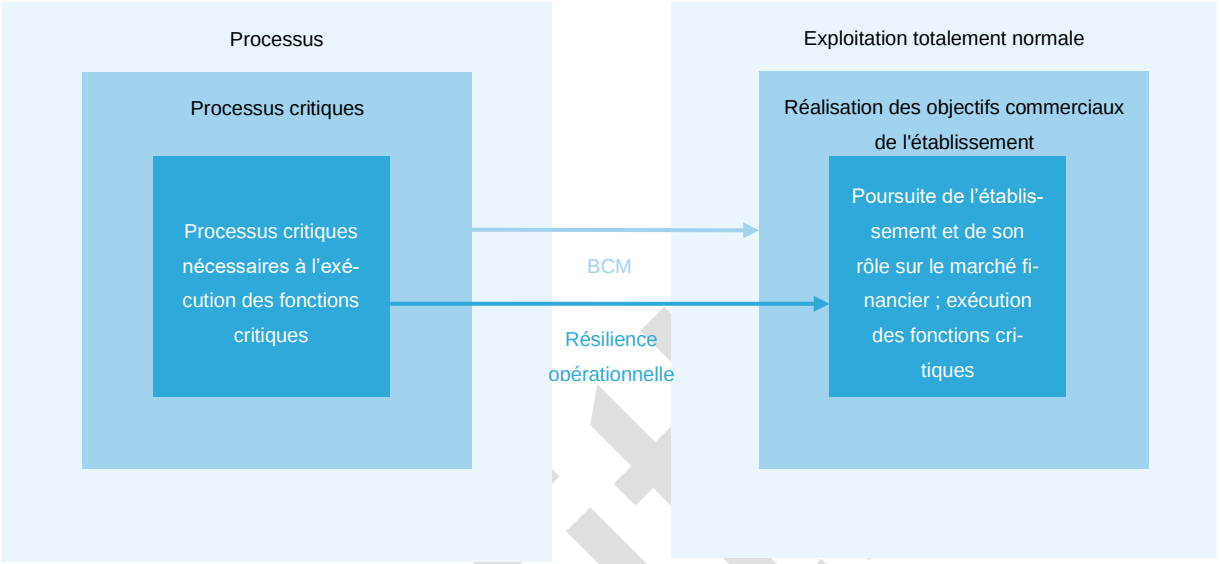
[19] Par ex. pandémie ou pénurie d'électricité.

paquet de révisions des normes finales de Bâle III et de l'ordonnance d'exécution FINMA correspondante.

Annexe 1

Graphiques explicatifs concernant la résilience opérationnelle

I. Chevauchement des objectifs de protection du BCM et de la résilience opérationnelle



II. Composantes pour l'exécution des fonctions critiques