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 2023/1
Risques et résilience opérationnels – banques

Gestion des risques opérationnels et garantie de la résilience opérationnelle

Référence :	Circ.-FINMA 23/1 « Risques et résilience opérationnels – banques »
Date :	7 décembre 2022
Entrée en vigueur :	1er janvier 2024
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. 1*b* al. 3 le. b, art. 3 al. 2 let. a et 3*f* OB art. 12 et 14*e* LEFin art. 9 et 49 OEFin art. 12 et 68
Annexe 1 :	Graphique explicatif 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 et 14*e* 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. Elle tient 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* et aux personnes selon l'art. 1*b* de la loi sur les banques (LB ; RS 952.0), 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 personnes selon l'art. 1*b* LB, les maisons de titres ainsi que les groupes et conglomérats financiers. 2

II. Définitions

Les *risques opérationnels* sont définis à l'art. 89 OFR. On entend par là le risque de pertes financières résultant de l'inadéquation ou de la défaillance de processus ou de systèmes internes, d'actions inappropriées de personnes ou d'erreurs qu'elles ont commises ou encore d'événements externes. Sont comprises les pertes financières qui peuvent découler des risques juridiques ou des risques de *compliance*. La gestion des risques opérationnels prend typiquement également en compte d'autres types de dommages[3], dans la mesure où ceux-ci peuvent aussi aboutir à des pertes financières. Les risques stratégiques en sont exclus. 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 qui, compte tenu de la taille, de la complexité, de la structure, du profil de risque ainsi que du modèle d'affaires de l'établissement revêtent une importance telle qu'elles nécessitent des exigences accrues en matière de sécurité. Ces données sont importantes pour la prestation réussie et durable des services de l'établissement ou à des fins réglementaires. Lors de l'évaluation et de la définition de la 7

[1] CBCB, « Revisions to the Principles for the Sound Management of Operational Risk » (31 mars 2021)

[2] CBCB, « Principles for Operational Resilience » (31 mars 2021)

[3] Par ex. répercussions négatives sur la réputation, perte potentielle de confiance et perte de clientèle, incidences négatives sur le marché, conséquences réglementaires négatives (par ex. perte potentielle de licence).

criticité des données, il faut prendre en compte la confidentialité, l'intégrité et la disponibilité. Chacun de ces trois aspects peut être déterminant pour classifier des données comme critiques.

Les *processus critiques* sont des processus qui, s'ils connaissent des incidents ou interruptions majeurs mettent en danger l'exécution des fonctions critiques. Ils font partie des fonctions critiques. 8

Le *business continuity management* (BCM) désigne l'approche adoptée à l'échelle de l'établissement pour rétablir le fonctionnement des processus critiques en cas d'incident ou d'interruption majeurs qui vont au-delà de la gestion des incidents. Il définit la réaction à un incident ou une interruption majeurs. Un BCM efficace diminue les risques résiduels liés aux incidents ou interruptions majeurs. 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 la TIC, en tenant compte de l'éventuelle indisponibilité de personnes clés. 12

Les *situations de crise* sont des situations exceptionnelles mettant potentiellement en danger l'existence de l'établissement et qui ne peuvent pas être maîtrisées à l'aide de mesures et compétences décisionnelles ordinaires. Elles se distinguent des incidents ordinaires ainsi que des incidents ou interruptions majeurs, qui peuvent être maîtrisés à l'aide de la gestion des incidents en situation normale ou des BCP et DRP définis. 13

Les *fonctions critiques* comprennent : 14

a. les activités, les processus et les services, y compris 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 15

b. les fonctions d'importance systémique selon l'art. 8 LB. 16

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. 17

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. Un établissement résilient sur le plan opérationnel a 18

établi son modèle d'exploitation[4] de manière à être moins exposé au risque d'interruptions de ses fonctions critiques. La résilience opérationnelle diminue non seulement les risques résiduels des interruptions, mais aussi le risque inhérent d'être soumis à une interruption. Une gestion efficace des risques opérationnels contribue à renforcer la résilience opérationnelle de l'établissement.

III. Principe de proportionnalité

La présente circulaire s'applique fondamentalement à l'ensemble de ses destinataires. Elle doit cependant être mise en œuvre au cas par cas en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement. La FINMA ordonne des allègements ou des renforcements au cas par cas. 19

Les banques et les maisons de titres des catégories FINMA 4 et 5 sont exemptées du respect des Cm 33 à 38, 41 à 46, 48, 51, 57, 73, 74, 76 à 78, 80, 87, 92, 93, 96, 103, 104 et 110 à 112. 20

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 72, 75, 79 ainsi que 105 à 109. 21

IV. Gestion des risques opérationnels

A. Gestion globale des risques opérationnels

La gestion des risques opérationnels fait partie de la gestion des risques à l'échelle de l'établissement conformément à la circulaire FINMA 2017/1 « Gouvernance d'entreprise – banques ». 22

L'organe responsable de la haute direction approuve l'approche pour la gestion des risques opérationnels pertinents pour l'établissement et surveille son respect. Sont inclus notamment les risques TIC, les cyberrisques, les risques des données critiques, les risques découlant de la conception et de la mise en œuvre du BCM et, le cas échéant, les risques liés aux activités de service transfrontières. Il approuve au moins une fois par année la tolérance au risque en matière de risques opérationnels en fonction de la politique de risque et 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 30. 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 à cet effet[5]. 23

L'organe responsable de la haute direction approuve régulièrement les stratégies de gestion des TIC, des cyberrisques, des données critiques et du BCM, et surveille leur respect. 24

La direction s'assure de manière compréhensible que les risques opérationnels sont identifiés, évalués, limités et surveillés et que l'efficacité tant de la conception que de la 25

[4] Souvent appelé *resilience by design*

[5] Par exemple un changement de modèle d'affaires

mise en œuvre de cette gestion des risques opérationnels est régulièrement vérifiée. Pour limiter les risques inhérents jugés importants[6], elle prend, en fonction de la situation, des mesures complémentaires spécifiques au risque ou renforce les mesures existantes.

Des mesures doivent être mises en œuvre[7] pour sensibiliser le personnel à la réduction des risques opérationnels pertinents, en particulier les risques TIC, les cyberrisques, les risques des données critiques et les risques découlant de la conception et de la mise en œuvre du BCM, en tenant compte de ses tâches, compétences et responsabilités. 26

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. Elle le fait avec retenue et en appliquant le principe de proportionnalité. 27

Les risques opérationnels doivent être catégorisés de façon uniforme à l'échelle de l'établissement et répertoriés dans un inventaire. Cette catégorisation peut s'appuyer sur la catégorisation des types d'événements utilisée dans le cadre du calcul des fonds propres minimaux pour les risques opérationnels ou sur une taxonomie interne. La catégorisation doit être appliquée de manière cohérente dans tous les domaines de l'établissement et dans toutes les composantes de la gestion des risques opérationnels. 28

Des facteurs internes[8] et externes[9] sont pris en compte dans l'identification des risques opérationnels. Les risques opérationnels identifiés sont évalués de manière compréhensible tant du point de vue des risques inhérents que des risques résiduels. 29

L'identification et l'évaluation des risques opérationnels s'appuient au moins sur les résultats d'audit[10] 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. 30

Pour évaluer les mesures de contrôle et d'atténuation existantes, une instance de contrôle indépendante procède à un examen régulier de l'efficacité des contrôles clés et le documente (*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, compétences et responsabilités pour garantir l'indépendance et prévenir les conflits d'intérêts fait l'objet d'évaluations régulières. 31

Des évaluations ad hoc des risques et des contrôles doivent être effectuées avant des changements importants dans les produits, les activités, les procédures et les systèmes. 32

---

[6] Appelés aussi risques principaux ou risques clés *(key risks)*

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

[8] 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.

[9] 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, de cyberattaques ou du terrorisme) ou les changements en matière d'exigences réglementaires.

[10] Les résultats d'audit comprennent ici 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 d'activité et d'organisation, le contrôle des risques, la fonction de *compliance* ou les autorités de surveillance.

Celles-ci prennent en compte les risques opérationnels découlant du processus de changement et les risques opérationnels de l'état cible. La tolérance au risque est adaptée si besoin et des mesures de contrôle et d'atténuation sont mises en œuvre.

En fonction de la nature, de l'ampleur, de la complexité et du risque des produits, activités, procédures et systèmes spécifiques à l'établissement, il s'agit d'appliquer les instruments et méthodes supplémentaires suivants : 33

a. la collecte et l'analyse systématiques des données de pertes internes et des événements externes pertinents liés à des risques opérationnels ; 34

b. les indicateurs de risque et de contrôle pour la surveillance des risques opérationnels et l'identification rapide des hausses de risque pertinentes ; 35

c. les analyses de scénario et/ou l'estimation du potentiel de perte compte tenu ou vis-à-vis des fonds propres minimaux pour les risques opérationnels ; 36

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. 37

La tolérance au risque pour les risques opérationnels tient compte de la tolérance en lien tant avec les risques inhérents[11] qu'avec les risques opérationnels résiduels. Elle fait l'objet d'une surveillance au moyen d'indicateurs de risque ou de contrôle. 38

Le rapport du contrôle des risques remis au moins une fois par année à l'organe responsable de la haute direction et au moins une fois par semestre à la direction selon les Cm 75 et 76 de la Circ.-FINMA 17/1 rend compte des risques opérationnels selon le niveau supérieur[12] de leur catégorisation définie conformément au Cm 28, de leur comparaison avec la tolérance aux risques fixée ainsi que des détails concernant les pertes internes importantes. 39

En ce qui concerne les risques TIC et les cyberrisques, le rapport remis au moins une fois par année à la direction contient en outre des informations sur l'évolution de ces risques, l'efficacité des contrôles clés correspondants et les événements importants internes et externes en lien avec ces risques. 40

Le rapport interne au sens du Cm 39 contient à titre complémentaire les informations suivantes : 41

- les facteurs externes pertinents selon la note de bas de page 9, 42
- la vue d'ensemble récapitulative sur l'efficacité des contrôles clés selon le Cm 31, 43
- les risques opérationnels émergents, 44
- les résultats découlant de l'application des instruments et des méthodes supplémentaires selon le Cm 33. 45

[11] La tolérance au risque par rapport aux risques inhérents tient compte de décisions stratégiques en lien avec le modèle d'affaires ou d'exploitation, par ex. la tolérance aux risques inhérents, qui peuvent découler d'activités avec certains pays ou segments de clientèle, de l'offre de certains produits, de l'application de processus majoritairement manuels, du recours à une infrastructure informatique complexe ou de certaines externalisations *(outsourcing)*.

[12] Le niveau supérieur de la catégorisation est souvent appelé niveau 1 ou *level 1.* Le rapport peut aussi être effectué de façon plus détaillée.

De plus, conformément au principe de proportionnalité, les banques d'importance systémique rendent compte régulièrement des risques opérationnels au niveau des domaines d'activité et d'organisation exposés à des risques opérationnels pertinents ou principaux. 46

B. Gestion des risques TIC

a) Stratégie TIC et gouvernance

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et de la sensibilisation aux TIC sont définies aux Cm 23 à 26 et 40. 47

La gestion des risques TIC tient compte des normes pertinentes et pratiques reconnues à l'échelle internationale ainsi que de l'influence des nouvelles évolutions technologiques sur les risques TIC. 48

La direction s'assure que des procédures, des processus, des contrôles ainsi que des tâches, compétences et responsabilités soient implémentés et documentés tant pour la gestion des changements *(change management)* que pour l'exploitation TIC *(run, maintenance)*. Ceux-ci sont dotés de ressources qualifiées et appropriées. 49

b) Gestion des changements *(change management)*

La gestion des changements définit des procédures, des processus et des contrôles pour toutes les phases de développement ou d'acquisition de TIC. Elle prend en compte dans chaque phase les conséquences du changement qui en découlent pour les risques TIC. Ce faisant, l'accent est mis notamment sur les exigences concernant la confidentialité, l'intégrité et la disponibilité. 50

Il faut garantir la séparation entre, d'une part, les environnements de développement ou de test et, d'autre part, l'environnement de production TIC. Cela comprend également une attribution claire de tâches, compétences et responsabilités ainsi qu'une réglementation des autorisations d'accès afférentes. 51

Lors du développement et de l'acquisition de TIC, les exigences fonctionnelles et non fonctionnelles[13] sont clairement définies et approuvées, puis testées et validées selon leur criticité. 52

c) Exploitation TIC *(run, maintenance)*

L'établissement dresse un ou plusieurs inventaire(s) 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 au sein de l'établissement ainsi que des interfaces avec les prestataires externes importants. 53

L'inventaire est disponible rapidement et est régulièrement revu et mis à jour en ce qui concerne son exhaustivité et sa véracité. 54

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 de la tolérance au risque correspondante. 55

[13] Par ex. en ce qui concerne l'architecture ou les exigences à l'égard de la sécurité de l'information

L'établissement garantit la transition irréprochable entre la gestion opérationnelle TIC et les procédures BCM et DRP en cas d'incidents ou interruptions majeurs. Il met en œuvre des procédures de sauvegarde et de restauration appropriées qui sont régulièrement testées et validées. 56

L'établissement dispose de procédures, de processus et de contrôles qui garantissent une gestion orientée vers le risque des TIC dont la fin d'exploitation approche ou dont la mise hors service prévue a été dépassée. 57

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 tient compte de l'ensemble du cycle de vie des incidents TIC importants et définit des tâches, compétences et responsabilités pour traiter ces incidents. 58

Le traitement des incidents TIC importants doit être coordonné et rattaché aux processus BCM et DRP. 59

Les établissements renseignent sans délai la FINMA sur les incidents TIC qu'ils considèrent comme des perturbations importantes pour l'exécution de leurs processus critiques et qui sont susceptibles de l'intéresser. 60

C. Gestion des cyberrisques

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les cyberrisques sont définies aux Cm 23 à 26 et 40. 61

L'établissement définit des tâches, compétences et responsabilités claires. Il 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 : 62

a. identification des menaces potentielles liées aux cyberattaques[14] spécifiques à l'établissement et évaluation des conséquences possibles liées à l'exploitation des vulnérabilités relatives aux composantes TIC répertoriées et des données électroniques critiques (selon Cm 53, 54 et 7) ; 63

b. protection des composantes TIC répertoriées et des données électroniques 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 ; 64

c. enregistrement et détection rapides des cyberattaques sur la base d'un processus de surveillance systématique et constant des composantes TIC répertoriées et des données électroniques critiques ; 65

[14] Attaques contre la confidentialité, l'intégrité et la disponibilité des TIC ainsi que les données électroniques critiques au moyen de l'exploitation des vulnérabilités ou du contournement des mesures protectrices par des cybercriminels externes ou internes.

d. réaction aux vulnérabilités et aux cyberattaques identifiées par le développement et l'implémentation de processus appropriés afin de prendre rapidement des mesures d'atténuation et de suppression ; et 66

e. garantie d'un rétablissement rapide de la marche ordinaire des affaires après des cyberattaques, grâce à des mesures appropriées. 67

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 composantes TIC répertoriées ainsi que les données électroniques critiques et les processus critiques (y compris les fonctions et services externalisés) et que l'obligation d'annoncer selon la LFINMA soit respectée. Après une première évaluation et une information préalable au service compétent de la FINMA dans les 24 heures, l'annonce doit être transmise dans les 72 heures, conformément au cahier des charges de la plate-forme de saisie EHP (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 au service compétent de la FINMA. 68

La direction fait régulièrement procéder à des analyses de vulnérabilité[15] et à des tests d'intrusion[16]. Ces derniers doivent être effectués par du personnel qualifié disposant de ressources adéquates. Ce faisant, toutes les composantes TIC répertoriées et accessibles par Internet doivent être prises en compte. En outre, les composantes TIC répertoriées et non accessibles par Internet mais qui sont nécessaires à l'exécution de processus critiques ou qui contiennent des données électroniques critiques, doivent être prises en compte. 69

Sur la base des menaces potentielles spécifiques à l'établissement, il y a lieu d'effectuer, en fonction des risques, des cyberexercices[17] fondés sur des scénarios. Le résultat des exercices doit être documenté et rapporté en forme appropriée. 70

D. Gestion des risques des données critiques

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les risques des données critiques sont définies aux Cm 23 à 26. 71

La direction définit des processus, des procédures et des contrôles adéquats ainsi que des tâches, compétences et responsabilités claires relatifs au traitement des données critiques identifiées par l'établissement. Par ailleurs, la direction mandate une unité pour créer et maintenir les conditions-cadres permettant de garantir la confidentialité, l'intégrité et la disponibilité des données critiques et de surveiller leur respect. 72

L'établissement identifie ses données critiques de manière systématique et exhaustive, les catégorise selon leur criticité et définit des responsabilités claires en matière de données. 73

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

[16] Évaluation ciblée et exploitation des vulnérabilités des logiciels et des failles de sécurité des TIC

[17] En tenant compte du Cm 19, ces cyberexercices pourraient par ex. inclure des exercices *table-top*, *red teaming*, etc.

Les données critiques définies par l'établissement sont gérées tout au long de leur cycle de vie. 74

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. 75

Durant l'exploitation et pendant le développement, le changement et la migration des TIC, l'accès et l'utilisation des données critiques doivent être protégés de manière appropriée vis-à-vis des personnes non autorisées. Cela s'applique également aux données critiques dans les environnements de test. 76

Les composantes TIC, qui sauvegardent ou traitent des données critiques, sont à protéger en particulier. L'accès à ces données doit être réglementé systématiquement et surveillé en permanence. 77

L'accès aux données critiques et aux fonctionnalités de traitement de ces données est limité aux personnes qui en ont besoin pour accomplir leurs tâches[18]. À cet égard, l'établissement doit disposer d'un système d'autorisation. L'accès à ce système doit être particulièrement protégé et régulièrement vérifié. Les autorisations contenues dans ce système doivent être régulièrement contrôlées. 78

Lorsque les données critiques sont stockées hors de Suisse[19] ou qu'elles sont accessibles depuis l'étranger, les risques accrus qui en résultent doivent être limités de manière appropriée et surveillés au moyen de mesures appropriées et les données doivent être particulièrement protégées. 79

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[20] et formées régulièrement sur le traitement de ces données. Des exigences accrues en matière de sécurité s'appliquent aux personnes bénéficiant de privilèges accrus[21]. Il convient en outre de tenir une liste de ces personnes et de la mettre continuellement à jour. 80

Les incidents qui entravent de manière importante la confidentialité, l'intégrité ou la disponibilité des données critiques doivent être annoncés immédiatement à la FINMA. 81

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 traiter[22]. Il faut définir des critères clairs pour évaluer la manière dont les prestataires gèrent les données critiques et les vérifier avant de signer des contrats. En fonction du risque, les prestataires doivent être soumis à une surveillance et à un contrôle périodiques dans le cadre du système de contrôle interne de l'établissement. 82

[18] Par ex. principe du *need-to-know* et du *least privilege*

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

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

[21] 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.

[22] Traiter : toute opération relative à des données critiques, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données

E. *Business continuity management* (BCM)

Les attentes fondamentales à l'égard de la stratégie, de la gouvernance et du renforcement de la prise de conscience en lien avec les risques découlant de la conception et de la mise en œuvre du BCM sont définies aux Cm 23 à 26. 83

Chaque domaine d'activité ou d'organisation pertinent doit identifier ses processus critiques et les ressources correspondantes nécessaires[23] dans le cadre de la *business impact analysis* (BIA). 84

Pour les processus critiques, l'établissement définit le RTO et le RPO conformément au Cm 10. Ceux-ci sont coordonnés avec les fournisseurs de prestations[24] 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. 85

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 84. L'acceptation des risques résiduels est documentée de manière adéquate. 86

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 revus et mis à jour chaque année ainsi qu'en cas de changements majeurs dans l'activité (réorganisations, création d'un nouveau champ d'activité, etc.). 87

L'établissement définit au moins un DRP en tant que partie intégrante du BCP. Lorsque des processus critiques ou des parties de ceux-ci sont externalisés, le DRP tient compte des dépendances externes et des dispositions contractuelles ainsi que des solutions alternatives. Le DRP est revu et mis à jour en cas de changements majeurs, mais au moins une fois par année. 88

Dans les situations de crise, un état-major de crise est chargé de gérer celle-ci jusqu'au rétablissement de la situation. Les événements déclencheurs d'une crise et les tâches, compétences et responsabilités de l'état-major de crise doivent être réglés au préalable. 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. 89

L'établissement définit une stratégie de communication interne et externe en situation de crise. 90

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 systématique afin de garantir une couverture régulière. Différentes manières de procéder au test avec des degrés d'intensité et d'efficacité variables peuvent être choisies, comme des exercices *table-top*. 91

[23] 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.

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

Les principales mesures du BCP et du DRP ainsi que l'organisation de crise sont testées au moins une fois par année. 92

Les parties prenantes, y compris celles issues des fonctions IT et des fonctions spécialisées, participent aux tests pour se familiariser aux processus de rétablissement. 93

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. 94

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. 95

Les collaborateurs ainsi que les membres de l'organisation de crise doivent être suffisamment formés au sujet de leurs tâches, compétences et responsabilités 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. 96

F. 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. 97

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 en question, définissent des modèles de prestations spécifiques aux pays desservis, forment le personnel et garantissent le respect des prescriptions grâce à des mesures organisationnelles, des directives et des modèles de rémunération et de sanction correspondants. 98

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. 99

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. 100

V. Garantie de la résilience opérationnelle

L'établissement identifie ses fonctions critiques et leurs tolérances aux interruptions. Celles-ci sont approuvées par l'organe responsable de la haute direction. En outre, l'organe responsable de la haute direction approuve et surveille régulièrement la procédure visant à garantir la résilience opérationnelle. 101

L'établissement prend des mesures pour garantir la résilience opérationnelle en tenant compte de scénarios graves, mais plausibles[25]. 102

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. 103

L'établissement coordonne les composantes pertinentes d'une gestion des risques globale, comme la gestion des risques opérationnels, y compris la gestion des risques TIC et des cyberrisques, le *business continuity management*, la gestion des externalisations (*outsourcing* ; cf. circulaire FINMA 2018/3 « Outsourcing ») et le plan d'urgence (chapitre VI), pour qu'elles contribuent à renforcer la résilience opérationnelle de l'établissement. Cela inclut un échange approprié des informations pertinentes entre ces différents domaines. 104

La direction et l'organe responsable de la haute direction doivent recevoir au moins une fois par année des rapports sur la résilience opérationnelle ainsi qu'en cas de faiblesses de contrôle importantes ou d'incidents qui menacent la résilience opérationnelle. 105

Pour les fonctions critiques, les menaces internes et externes 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. 106

L'établissement constitue un inventaire de ses fonctions critiques, qui doit être revu 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[26] pour exécuter les fonctions critiques. 107

Pour les fonctions critiques, l'établissement documente au minimum les risques opérationnels importants et les contrôles clés . 108

Les fonctions critiques et les processus critiques et ressources nécessaires à cet effet sont couverts par les BCP selon le chapitre IV lettre E. 109

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 ou exercée. Il s'agit notamment de scénarios qui se distinguent des interruptions brèves et plutôt limitées en se démarquant par des interruptions de longue durée (par ex. plusieurs mois) 110

[25] Il ne peut être exclu que certains scénarios ne puissent pas être gérés sans intervention de l'État (par ex. pandémies, guerres, pénuries d'électricité durables). Pour de tels scénarios, l'établissement doit effectuer des travaux préparatoires pour renforcer sa résilience opérationnelle dans le cadre de ses possibilités.

[26] Y compris les composantes de l'inventaire pertinentes pour les fonctions critiques selon le Cm 53

et la défaillance de ressources fondamentales[27]. Les tests ou exercices sont conçus de sorte à ne pas menacer fondamentalement l'établissement.

S'agissant des banques d'importance systémique, le BCP, le DRP et l'organisation en cas de crise selon le chapitre IV lettre E, pertinents pour la poursuite des fonctions critiques selon le Cm 14, doivent être coordonnés avec leur plan d'urgence selon le chapitre VI. 111

VI. 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 lien avec les art. 60 ss OB). Elles identifient les prestations requises 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. 112

VII. Dispositions transitoires

A. À propos de la garantie de la résilience opérationnelle

L'identification des fonctions critiques, la définition des tolérances aux interruptions et les premières approbations selon les Cm 101 et 103 ainsi que le premier rapport selon le Cm 105 sont attendus dès l'entrée en vigueur de la présente circulaire. Un délai transitoire d'une année à compter de l'entrée en vigueur est applicable pour satisfaire aux exigences selon les Cm 106 à 109 ainsi qu'effectuer les premiers tests selon le Cm 110. La garantie de la résilience opérationnelle selon le Cm 102 ainsi que la satisfaction des exigences selon les Cm 104 et 111 sont attendues dans un délai transitoire de deux ans. 113

B. À propos des exigences de fonds propres pour les risques opérationnels

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 de l'OFR révisée dans le cadre du paquet de révisions des normes finales de Bâle III et de l'ordonnance d'exécution FINMA correspondante. 114

[27] Par ex. pandémie, pénurie d'électricité, défaillance prolongée en raison de l'insolvabilité d'un prestataire important (comme exemple de *stressed exit* d'un prestataire) ou interdiction persistante de la part de gouvernements étrangers aux fournisseurs de *cloud* ou d'autres prestataires basés à l'étranger de servir des entreprises suisses.

Annexe 1

Graphique explicatif concernant la résilience opérationnelle

Composantes nécessaires à l'exécution des fonctions critiques