Loi sur les banques

Dernière modification : 23.08.2026

PDF créé le : 05.10.2026

COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

TABLE DES MATIÈRES

Art. 1b LB 5

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 1b LB

Un commentaire de Tamara Teves / David Meirich

PROPOSITION DE CITATION

Tamara Teves/David Meirich, Commentaire de l'art. 1b LB., in: Nina Reiser/Beat Brändli (édit.), Commentaire en ligne de la Loi sur les banques

Citation abrégée: OK-Teves/Meirich, art. 1b LB N. XXX.

Art. 1*b* Promotion de l'innovation

[1] Les dispositions de la présente loi s'appliquent par analogie aux personnes qui sont principalement actives dans le secteur financier et qui:

a. acceptent à titre professionnel des dépôts du public jusqu'à concurrence de 100 millions de francs ou des cryptoactifs désignés par le Conseil fédéral, ou font appel au public pour les obtenir, et

b. n'investissent ni ne rémunèrent ces dépôts ou actifs.

[2] Le Conseil fédéral peut adapter le montant fixé à l'al. 1. Ce faisant, il tient compte de la compétitivité et de la capacité d'innovation de la place financière suisse.

[3] Les personnes visées à l'al. 1 doivent notamment:

a. définir exactement leur champ d'activité et prévoir une organisation correspondant à cette activité;

b. disposer d'une gestion des risques aménagée de manière adéquate et d'un contrôle interne efficace, qui garantit notamment le respect des prescriptions légales et internes à l'entreprise (compliance);

c. disposer de ressources financières adéquates;

d. garantir que les personnes chargées de l'administration et de la gestion jouissent d'une bonne réputation et présentent toutes les garanties d'une activité irréprochable.

4 Les dispositions suivantes sont réservées:

a. les comptes des personnes visées à l'al. 1 sont établis exclusivement selon les prescriptions du code des obligations (CO);

b. les personnes visées à l'al. 1 doivent faire contrôler leurs comptes annuels et, le cas échéant, leurs comptes consolidés conformément aux prescriptions du CO; l'art. 727*a*, al. 2 à 5 CO ne s'applique pas;

c. les personnes visées à l'al. 1 chargent une société d'audit agréée par l'Autorité fédérale de surveillance en matière de révision selon l'art. 9*a*, al. 1 ou 4bis, de la loi du 16 décembre 2005 sur la surveillance de la révision[14] de procéder à un audit conformément à l'art. 24 de la loi du 22 juin 2007 sur la surveillance des marchés financiers (LFINMA);

d. les dispositions sur les dépôts privilégiés (art. 37*a*) et le remboursement immédiat (art. 37*b*) ne s'appliquent ni aux dépôts du public ni aux cryptoactifs désignés par le Conseil fédéral détenus auprès des personnes visées à l'al. 1; les déposants doivent être informés de cette restriction avant d'effectuer le dépôt.

5 Dans des cas particuliers, la FINMA peut déclarer les al. 1 à 4 applicables aux personnes qui acceptent à titre professionnel des dépôts du public supérieurs à 100 millions de francs ou font appel au public pour les obtenir, n'investissent ni ne rémunèrent ces dépôts et garantissent la protection des clients par des mesures particulières.

[6] Quiconque dépasse le seuil de 100 millions de francs doit l'annoncer dans les dix jours à la FINMA et lui présenter une demande d'autorisation au sens de l'art. 1*a* dans les 90 jours. L'al. 5 est réservé.

TABLE DES MATIÈRES

I. Introduction 11
II. Procédure d'autorisation 12
A. Examen préliminaire 12
B. Examen de la demande 14
C. Décision d'autorisation 17
III. Champ d'application (al. 1 et 2) 18
A. Acceptation de dépôts du public (al. 1, let. a) 18
B. Conservation collective d'actifs cryptographiques (al. 1, let. a) 18
C. Interdiction de placement et de rémunération (al. 1, let. b) 19
D. Adaptation du seuil applicable aux dépôts du public par le Conseil fédéral (al. 2) 21
IV. Conditions d'autorisation (al. 3 et 4) 21
A. Champ d'activité (al. 3, let. a) 21
1. Généralités 21
2. Conservation des dépôts du public et des actifs cryptographiques (al. 3, let. a) 24
a. Conservation des dépôts du public 24
b. Surveillance du seuil applicable aux dépôts du public (al. 6) 27
3. Conservation des actifs cryptographiques 27
B. Organisation administrative appropriée (al. 3, let. a) 29
1. Forme juridique, siège et lieu d'activité 29
2. Organes 31
3. Infrastructure et personnel 32
a. Locaux commerciauxux 32
b. Ressources humaines 32
c. Infrastructure technique 33
4. Externalisation 33
a. Possibilité d'externalisation 33
b. Caractère significatif 34
c. Inventaire 36
d. Analyse des risques 36
e. Sélection, instruction et contrôle du prestataire 36
f. Audit et surveillance 36
g. Contrats d'externalisation 37
h. Rapports 38
i. Situations au sein du groupe 39
j. Responsabilité et sécurité 39
k. Externalisation à l'étranger 39
l. Conditions et exceptions 39

C. Gouvernance d'entreprise : gestion des risques, contrôles internes et conformité (al. 3, let. b) ... 40
1. Principes fondamentaux ... 40
2. Fonctions de contrôle indépendantes ... 42
3. Gestion des risques ... 43
a. Responsabilités ... 43
b. Inventaire ... 44
c. Identification ... 44
d. Tolérance au risque ... 45
e. Formation du personnel ... 45
f. Contrôle ... 46
g. Rapports ... 46
h. Risques liés aux TIC ... 47
a. Stratégie et gouvernance ... 47
b. Gestion des changements ... 47
c. Exploitation des TIC ... 47
d. Gestion des incidents ... 48
i. Risques cybernétiques ... 48
j. Risques liés aux données critiques ... 51
k. Gestion de la continuité des activités ... 52
l. Risques liés aux activités transfrontalières de prestation de services ... 53
m. Résilience opérationnelle ... 54
4. Service spécialisé dans la lutte contre le blanchiment d'argent ... 55
5. Documentation et processus ... 56
6. Prévention des conflits d'intérêts ... 57
D. Exigences financières (al. 3, let. c) ... 57
1. Plan d'affaires ... 57
2. Liquidité ... 59
3. Capital minimum ... 59
E. Garantie (al. 3, let. d) ... 60
F. Présentation des comptes et révision comptable (al. 4, let. a, b et c) ... 64
G. Obligations d'information (al. 4, let. d) ... 64
V. Cas particuliers (y compris les al. 5 et 6) ... 66
A. Augmentation éventuelle du seuil applicable aux dépôts du public par la FINMA (al. 5 et 6) ... 66
B. Combinaison avec d'autres catégories d'autorisation ... 66
C. Surveillance consolidée ... 67
D. Situations transfrontalières ... 71
1. Activité à l'étranger (outbound) ... 71
2. Contrôle étranger ... 72
3. Représentations (inbound) ... 73

VI. Modifications de l'autorisation 74
VII. Historique des autorisations 76
VIII. Évolution de l'autorisation dans le domaine de la fintech 77
Bibliographie 78
Matériaux 80

I. INTRODUCTION

Le présent art. 1*b* a été intégré à la loi sur les banques (LB) par le Parlement le 15 juin 2018 – dans le cadre des dispositions relatives à la **promotion de l'innovation** – en même temps que la loi sur les services financiers et la loi sur les établissements financiers. Toutes ces dispositions relatives à la promotion de l'innovation sont entrées en vigueur le 1er janvier 2019. 1

Le **secteur de la fintech** est en constante évolution. Les modèles économiques de ce secteur évoluent donc également en conséquence. Afin de tenir compte de cette réalité, la catégorie d'autorisation visée à l'art. 1*b*, al. 1 de la LB ne se limite ni à certains modèles économiques de la fintech, ni au secteur de la fintech en tant que tel. Si la nouvelle réglementation visait principalement à réduire les obstacles à l'entrée sur le marché pour les entreprises de fintech, la disposition est toutefois formulée de manière ouverte et s'applique de manière générale à toutes les personnes exerçant une activité dans le secteur financier. Ainsi, en principe, des entreprises n'appartenant pas au secteur de la fintech peuvent également obtenir une autorisation au titre de l'art. 1 *b* de la Loi sur les banques (LB), pour autant qu'elles remplissent les conditions légales. Ce champ d'application ouvert transparaît également dans le titre de la disposition légale («Promotion de l'innovation»). Malgré ce champ d'application ouvert, l'accent est toutefois mis, dans la pratique, sur le secteur de la fintech. Une innovation particulière n'est toutefois pas exigée dans le cadre de cette catégorie d'autorisation. 2

Les modèles économiques des établissements fintech nécessitent parfois la **collecte de dépôts du public** (ce que l'on appelle les opérations de passif). L'exercice simultané d'opérations d'actif (et donc des opérations sur les marges d'intérêt) doit toutefois rester réservé aux banques, même après l'introduction des dispositions relatives à la promotion de l'innovation. C'est pourquoi un établissement fintech n'est pas autorisé à placer les fonds collectés ni à leur verser des intérêts (cf. art. 1*b*, al. 1, let. b, LB). 3

Avant l'adoption de l'art. 1*b* LB, la collecte à titre professionnel de dépôts du public était exclusivement réservée aux **banques**. L'exercice d'une telle activité sans autorisation bancaire était punissable (cf. art. 46, al. 1, let. a, et art. 49, al. 1, let. c, LB). Les établissements fintech visés en particulier par cette 4

réglementation fournissent des services assimilables à ceux des banques, mais ne relèvent pas de l'activité principale de ces dernières.

5En Suisse, de nombreux services (tant les services de paiement que le négoce et la conservation individuelle d'actifs cryptographiques) – pour autant que leur activité ne soit pas couverte par d'autres textes législatifs relatifs au droit des marchés financiers – sont possibles même sans autorisation de l'Autorité fédérale de surveillance des marchés financiers (FINMA), mais sous la surveillance d'un OAR en matière de lutte contre le blanchiment d'argent. Ainsi, certains services de paiement ainsi que le négoce et la conservation individuelle de crypto-actifs peuvent être proposés sous la surveillance d'un OAR (on estime actuellement à environ 200 le nombre de prestataires de services liés aux cryptomonnaies et à environ 50 celui des prestataires de services de paiement soumis à la surveillance d'un OAR). Il convient de tenir compte de ce contexte lorsqu'on évalue le nombre de nouveaux prestataires. Le régime d'autorisation « fintech » prévu à l'art. 1*b* de la LB s'adresse donc à un profil de modèle d'affaires très spécifique : les établissements qui acceptent et transfèrent des dépôts du public (fonds de la clientèle) (services de paiement).

6 Le respect des exigences d'autorisation est contrôlé dans le cadre d'une surveillance continue exercée par la FINMA, qui est également compétente pour sanctionner les comportements fautifs sur le plan prudentiel, tels que l'exercice d'une activité soumise à autorisation sans autorisation.

II. PROCÉDURE D'AUTORISATION

A. Examen préliminaire

7 La FINMA procède, pour les projets susceptibles de déboucher sur une procédure d'autorisation pour des établissements de fintech (comme c'est le cas pour les banques et les maisons de courtage), procède à un examen préliminaire. Cet **examen préliminaire** doit permettre à la FINMA de se familiariser avec les grandes lignes du projet et de procéder à un premier état des lieux réglementaire. Les initiateurs du projet peuvent ainsi obtenir très tôt des indications sur d'éventuels obstacles à l'autorisation ou aborder directement avec la FINMA les questions qui leur semblent essentielles.

8En vue d'une première prise de contact, il convient de soumettre à la FINMA une **présentation du projet** qui doit contenir au moins les informations suivantes :

- modèle économique et description de l'activité soumise à autorisation ;
- acteurs clés du projet (c'est-à-dire les personnes impliquées qui, le cas échéant, assumeront ultérieurement un rôle de « garant ») ;
- les ressources financières du projet et l'origine des fonds (sur la base de chiffres actualisés) ;
- l'organisation prévue ;
- si le projet fait partie d'un groupe : aperçu de la structure du groupe ;
- toute indication relative à des faits dignes d'être mentionnés qui pourraient revêtir une importance pour la procédure d'autorisation (par exemple, des procédures à l'encontre de garants potentiels) ;
- calendrier ;
- procuration (en cas de représentation).

En résumé, la présentation du projet doit donner à la FINMA une première idée de la composition du projet en termes de personnel, de ressources financières et d'organisation. 9

Après réception de la présentation du projet, la FINMA décide de l'opportunité d'organiser une réunion. Certaines questions relatives au contexte d'autorisation, dont les réponses revêtent une importance particulière pour le fond de l'affaire, peuvent, sur demande, être traitées dans le cadre d'une **question préalable**. Les présentations de projet doivent être adressées au Fintech-Desk de la FINMA dans l'une des langues officielles ou en anglais. 10

Si, dans le cadre de l'examen préliminaire, la FINMA parvient à la conclusion que le projet présenté n'est probablement pas **éligible à une autorisation**, que ce soit par exemple en raison d'un manque de moyens financiers suffisants, d'une provenance des fonds non vérifiable, en raison de l'impossibilité d'exercer une surveillance consolidée, du manque de qualifications des personnes impliquées en tant que futurs garants ou d'une présence insuffisante en Suisse, il est déconseillé de déposer une demande d'autorisation. Dans ce cas, les initiateurs du projet ont la possibilité de 11

soumettre un nouveau projet préliminaire, à condition que les aspects soulevés lors de l'entretien soient traités de manière appropriée et que les justificatifs correspondants puissent être fournis.

12 Si la FINMA estime que le projet présenté est susceptible d'être autorisé, le demandeur est informé de la possibilité de déposer la **demande d'autorisation**. La demande préalable doit être simple et peu coûteuse. Elle ne fait donc pas l'objet d'une procédure administrative formelle aboutissant à une décision. Elle peut plutôt être considérée comme un service de clarification préalable fourni par la FINMA.

13 Les clarifications relatives aux projets d'autorisation sont soumises à des émoluments. L'**émolument** est fixé conformément à l'ordonnance de la FINMA sur les émoluments et les taxes (OEMOL-FINMA).

B. Examen de la demande

14 Une fois l'examen préalable conclu avec succès et en présence d'un rapport d'autorisation, la **demande d'autorisation** correspondante peut être déposée auprès de la FINMA.

15 Conformément au système de double surveillance, la FINMA exige en principe, dans le cadre de la procédure d'autorisation, que le requérant présente un **rapport d'audit d'autorisation** établi par une société d'audit disposant d'une agrément correspondant à l'art. 9a de la loi sur la surveillance de la révision (LSR). La nécessité d'un tel rapport doit être appréciée au cas par cas ; toutefois, un rapport d'audit est exigé par défaut. Les rapports d'audit des différentes sociétés d'audit présentent parfois des différences considérables en termes de qualité (niveau d'approfondissement de l'audit) et de coûts, ce dont la requérante doit tenir compte lors de son choix. Plus le rapport est de haute qualité, plus il sera utile dans le cadre du traitement ultérieur de la demande par la FINMA. La durée de la procédure d'autorisation dépend en fin de compte de la complexité du projet ainsi que de la qualité et de l'exhaustivité de la demande.

16 Les **directives de la FINMA** relatives aux attestations à fournir par les sociétés d'audit dans le cadre des demandes d'autorisation en tant que personnes au sens de l'art. 1*b* de la Loi sur les banques (LB) s'adressent aux sociétés d'audit en ce qui concerne les demandes d'autorisation émanant d'établissements fintech nouvellement créés. Ces directives énumèrent les

attestations requises et les domaines d'audit que les sociétés d'audit, en leur qualité de contrôleurs d'autorisation, doivent au minimum couvrir dans le cadre d'une procédure d'autorisation. Elles n'excluent pas que les sociétés d'audit fournissent des informations supplémentaires ou que la FINMA exige d'autres informations et attestations.

Dans la mesure où un audit d'agrément est exigé – ce qui est généralement le cas –, la requérante doit joindre à sa demande d'autorisation une déclaration d'acceptation de la part de la **société d'audit chargée de l'examen d'autorisation** ainsi que le questionnaire rempli concernant les prestations des sociétés d'audit agréées. 17

La FINMA est compétente pour l'octroi de l'autorisation fintech. Lors de l'examen des demandes d'autorisation correspondantes, l'autorité de surveillance évalue si l'activité envisagée est soumise à autorisation et si elle est possible dans le cadre de l'autorisation « Fintech ». Afin de faciliter la procédure d'autorisation, la FINMA a publié un guide à l'intention des demandeurs. Celles-ci précisent notamment quels documents doivent être joints à la demande. 18

La demande doit être rédigée dans une **langue officielle ou en anglais**, les statuts, le règlement d'organisation ainsi que tout autre document de nature sociétaire soumis à autorisation devant être fournis dans une langue officielle suisse. La FINMA n'accepte pas les statuts ni le règlement d'organisation rédigés en anglais. Dans la pratique, ces documents relevant du droit des sociétés sont généralement rédigés en deux langues, ce que la FINMA accepte jusqu'à présent. Si une demande est déposée par un représentant légal, sa procuration doit être jointe au dossier. 19

Dès réception de la demande, la FINMA indique au demandeur quel collaborateur de la FINMA est chargé de la **procédure d'autorisation** et quelles informations et pièces justificatives supplémentaires doivent éventuellement être fournies ultérieurement. 20

L'autorité de surveillance peut effectuer elle-même ou faire effectuer l'**examen d'autorisation**, comme tous les autres examens (cf. art. 24, al. 1, de la loi sur la surveillance des marchés financiers [LFINMA] en liaison avec l'art. 2, al. 2, de l'ordonnance sur les contrôles des marchés financiers [O-FINMA]). L'examen porte sur le respect des dispositions prudentielles et sur la vérification que les conditions requises sont remplies ou pourront l'être dans 21

un avenir prévisible (art. 2, al. 1, O-FINMA) . L'examen porte notamment sur les risques que l'entité soumise à surveillance est susceptible de faire peser sur les créanciers ainsi que sur le bon fonctionnement des marchés financiers. Les doublons dans le cadre de l'examen doivent être évités dans la mesure du possible (art. 24, al. 2, LFINMA).

22 La FINMA veille notamment, dès la phase d'examen préliminaire, à ce que les **obstacles fondamentaux à l'octroi de l'autorisation** soient identifiés à un stade précoce. Dès que toutes les informations et tous les documents pertinents sont disponibles, la FINMA examine la demande et décide si l'autorisation peut être octroyée. Le requérant a l'obligation de coopérer pour compléter l'état des faits et apporter la preuve que les conditions d'octroi de l'autorisation sont remplies. L'autorisation demandée est accordée lorsque toutes les conditions d'octroi sont remplies sans aucun doute ou peuvent l'être.

23 La **durée de traitement** de la demande d'autorisation dépend de la qualité et de la complexité de la demande ainsi que des échanges avec les requérants. Pour les demandes présentant un lien particulièrement marqué avec l'étranger, comme par exemple l'appartenance à un groupe comprenant déjà des entreprises étrangères du secteur financier ou l'implication de personnes ayant déjà attiré l'attention des autorités étrangères de surveillance des marchés financiers par le passé, il convient en outre de tenir compte du délai de réponse des autorités de surveillance étrangères concernées.

24 **B Les facteurs**B qui entraînent des procédures d'autorisation longues peuvent également se combiner entre eux :

- préparation insuffisante des demandes d'autorisation (par exemple, description insuffisamment concrète de l'activité prévue, documentation lacunaire ou erronée) ;
- modifications apportées aux demandes d'autorisation par les requérants pendant l'examen en cours par la FINMA (par exemple, modification des activités commerciales prévues et/ou de l'organisation, changements au niveau des garants) ;
- de nombreux éléments accroissant la complexité (par exemple, garanties douteuses quant à la bonne conduite des activités des personnes concernées, rejet antérieur d'une demande d'autorisation de la requérante par une autorité de surveillance étrangère, origine peu claire des fonds

destinés au financement de la société, plans d'affaires ou de financement manifestement irréalistes).

La FINMA examine actuellement la mise en place d'une **«procédure accélérée»** pour les projets bien préparés, dans lesquels les risques sont traités de manière appropriée, afin que ceux-ci ne pâtissent pas de l'importante mobilisation de ressources nécessaire pour les autres demandes d'autorisation. Cela vise à éviter que la durée de traitement des demandes d'autorisation bien préparées et moins complexes ne soit également allongée en raison de cette mobilisation de ressources. 25

C. Décision d'autorisation

La FINMA clôt la procédure d'autorisation par une **décision d'autorisation**. La décision se compose d'un exposé des faits, d'un exposé des motifs et d'un dispositif. Alors que l'exposé des faits présente l'organisation du requérant, l'exposé des motifs fait référence au respect des conditions d'autorisation applicables dans chaque cas. Dans le dispositif, la FINMA prononce l'octroi de l'autorisation, ce qui se fait généralement sous réserve d'une prise d'effet différée liée au respect préalable de charges et de conditions. Ces charges et conditions comprennent généralement la signature de contrats de travail ou d'externalisation, la mise en vigueur de directives et de règlements, la présentation d'un exemplaire valablement signé du règlement d'organisation et d'exploitation, ainsi que la présentation des actes authentiques relatifs à la décision de l'assemblée générale concernant l'adoption du projet de statuts, l'élection en suspens des membres du conseil d'administration et l'élection de l'organe de révision. 26

L'autorisation devient normalement caduque si les conditions mentionnées dans le dispositif de la décision ne sont pas remplies dans un **délai d'un an** à compter de l'entrée en vigueur de la décision et si la requérante n'a pas été inscrite au registre du commerce en tant que personne au sens de l'art. 1*b* LB. L'autorisation devient en outre caduque si la requérante ne commence pas son activité nouvellement autorisée (acceptation de dépôts du public et/ou conservation collective d'actifs cryptographiques) dans un délai d'un an à compter de l'entrée en vigueur de la présente décision. Un recours contre la décision d'autorisation peut être formé dans un délai de 30 jours devant le Tribunal administratif fédéral (art. 54, al. 1, LFINMA en liaison avec l'art. 33, let. e, de la loi sur les tribunaux administratifs (LTAF)). 27

III. CHAMP D'APPLICATION (AL. 1 ET 2)

A. Acceptation de dépôts du public (al. 1, let. a)

28 L'art. 1*b* de la LB a créé une nouvelle catégorie d'autorisation pour les établissements qui acceptent à titre professionnel des dépôts du public à concurrence de 100 millions de francs suisses sans exercer d'activité de crédit (dite « autorisation fintech »). Les conditions d'octroi de cette autorisation ont été précisées par le Conseil fédéral dans le cadre d'une révision partielle de l'ordonnance sur les banques (OB), entrée en vigueur le 1er janvier 2019.

B. Conservation collective d'actifs cryptographiques (al. 1, let. a)

29 Avec l'entrée en vigueur, au 1er août 2021, de la loi fédérale du 25 septembre 2020 adaptant le droit fédéral aux évolutions techniques des registres électroniques distribués, août 2021, le **champ d'application** de l'autorisation « fintech » a été élargi.

30 Conformément à l'art. 1*b*, al. 1, let. a, LB, relève désormais également de l'autorisation « fintech » toute personne qui, à titre professionnel, accepte des **actifs cryptographiques** (conservés en dépôt collectif) désignés par le Conseil fédéral conformément à l'art. 5*a* OB.

31 Les actifs cryptographiques sont des actifs détenus en dépôt collectif au sens de l'art. 16, ch. 1bis, let. b, LB, qui servent, de fait ou selon l'intention de l'organisateur ou de l'émetteur, dans une large mesure de moyen de paiement pour l'acquisition de biens ou de services ou pour le transfert d'argent ou de valeurs, c'est-à-dire des **jetons de paiement** (hybrides) (art. 5*a*, al. 1, OB).

32 Dans le cadre de la **conservation collective**, l'établissement fintech est tenu de tenir les jetons de paiement à la disposition du client à tout moment, les jetons étant affectés à une communauté et il est possible de déterminer (au moyen d'une blockchain ou d'un registre interne) quelle part de l'actif commun (c'est-à-dire une adresse blockchain commune) revient à chaque client (art. 16, al. 1bis, let. b, LB).

33 La **conservation individuelle** de jetons de paiement sur une adresse blockchain individuelle au sens de l'art. 16, al. 1bis, let. a, LB n'entre donc pas dans le champ d'application de l'autorisation fintech. Il en va de même pour la

conservation de jetons d'utilisation ou d'investissement, c'est-à-dire de jetons sans fonction de paiement (hybride).

Une **autorisation** au sens de l'art. 1*b* LB peut donc être obtenue, d'une part, par toute personne qui, à titre professionnel, accepte du public des dépôts à hauteur de 100 millions de CHF ou des actifs cryptographiques désignés par le Conseil fédéral, ou qui recommande publiquement l'acceptation de tels dépôts ou actifs cryptographiques, et, d'autre part, qui n'investit ni ne rémunère ces dépôts du public ou ces actifs cryptographiques. L'autorisation est octroyée lorsque les conditions d'octroi prévues par le droit bancaire en vertu de l'art. 1*b* LB sont remplies. 34

C. Interdiction de placement et de rémunération (al. 1, let. b)

L'**interdiction de placement et de rémunération** au sens de l'art. 1*b*, al. 1, let. b, LB équivaut de fait à une interdiction d'octroi de crédits, c'est-à-dire à une interdiction des opérations actives. Seuls les modèles économiques qui renoncent aux opérations actives relèvent donc de la catégorie d'autorisation des établissements fintech. Dans ces cas, la licence « fintech » ne permet pas d'exercer l'activité typique des banques consistant à tirer profit des écarts de taux d'intérêt. 35

La notion de **placement** doit ici être comprise au sens très large. Étant donné que les fonds ne peuvent pas être placés, il faut partir du principe qu'ils sont conservés en permanence sous forme de liquidités sur les comptes de l'entreprise concernée (cf. art. 14*f*, al. 2 OB), qu'ils seront transférés conformément à l'accord conclu avec la clientèle ou – si ce n'est pas l'objectif visé ou si cela n'est pas possible – remboursés à la clientèle. Il est donc interdit aux titulaires d'autorisation d'exercer l'activité de marge d'intérêt réservée aux banques et de générer des bénéfices à partir de la différence entre les taux d'intérêt créditeurs et débiteurs. L'interdiction de placement signifie également que les dépôts ne peuvent pas être investis (en leur propre nom et pour leur propre compte) dans des produits de placement. 36

À cet égard, l'interdiction de placement et de rémunération a, dans la pratique, les **conséquences** suivantes : 37

- Les établissements fintech ne sont pas autorisés à accorder à leurs clients **des crédits** financés par des dépôts du public. Cela interdit également les découverts bancaires et les situations similaires, ainsi que le

préfinancement intrajournalier des transactions des clients (par exemple dans le domaine du change ou des paiements internationaux) au moyen de dépôts du public. Il convient donc de clarifier au cas par cas comment les prestataires de services tiers concernés facturent les frais de transaction et de tenue de compte ainsi que les préfinancements et marges de transaction, par exemple si les montants versés quotidiennement sont financés par les fonds de la société ou par des dépôts du public ;

- sont également interdites les **avances** sur fonds propres destinées au règlement des transactions des clients. Les avances intrajournalières sur fonds propres destinées au règlement des transactions des clients ne sont possibles, le cas échéant, que dans le cadre de l'exception prévue à l'art. 5, al. 3, let. a, OB ;
- **B les opérations de change à terme**B ne peuvent en principe pas être proposées par un établissement fintech, car les risques de capital et de liquidité qui y sont liés exigeraient au moins des exigences similaires à celles applicables aux banques ;
- la répercussion des **intérêts négatifs** est possible, mais pas celle des intérêts positifs sur les dépôts en compte courant auprès de la BNS ;
- **les produits de crédit** dans le domaine des cryptomonnaies ne peuvent pas être proposés avec l'autorisation fintech ;
- **le « custodial staking »** est soumis à une autorisation bancaire, sous réserve des exceptions prévues aux articles 5, 5*a* et 6 de l'ordonnance sur les banques (OB), dans la mesure où le staking conduit à une rémunération de facto (récompenses de staking), ce qui serait contraire à l'interdiction de rémunération ; à titre alternatif, les « Staking Rewards » pourraient également être considérées comme des frais de service, ce qui permettrait aux établissements fintech de proposer le « staking de dépôt », à condition que les exigences de la communication de surveillance FINMA 08/2023 « Staking » soient respectées à tout moment en ce qui concerne les actifs cryptographiques mis en staking. La doctrine nie l'existence d'une violation de l'interdiction de rémunération lors du versement de récompenses de staking aux clients.
- Les **plateformes de négociation de CFD** bilatérales sont en principe considérées comme des systèmes de négociation organisés (OHS) bilatéraux au sens de la loi sur les infrastructures des marchés financiers

(LIMF). Cette qualification en tant qu'activité OHS implique qu'une autorisation en tant que banque, maison de courtage, système de négociation DLT ou place de négociation (bourse, MHS) est requise (art. 43, al. 1, LIMF). Une autorisation « fintech » ne suffit donc pas à cet effet.

D. Adaptation du seuil applicable aux dépôts du public par le Conseil fédéral (al. 2)

Le Conseil fédéral peut adapter le montant de **100 millions de CHF** en tenant compte de la compétitivité et de la capacité d'innovation de la place financière suisse (art. 1*b*, al. 2, LB). Dans des cas particuliers justifiés, la FINMA doit également avoir la possibilité de déroger au plafond de 100 millions de CHF (art. 1*b*, al. 5, LB). 38

Dans ce cadre, le Conseil fédéral a annoncé en 2022 qu'il convenait d'examiner s'il fallait maintenir la **limite** de 100 millions de francs suisses pour l'acceptation des fonds des clients. Même si la FINMA peut, en vertu de l'art. 1*b*, al. 5 de la LB, cette restriction engendre des incertitudes quant à la manière dont la FINMA statuera en fin de compte. Les critères utilisés par la FINMA pour accorder une dérogation dans un cas particulier n'ont pas encore été publiés. Le Conseil fédéral ne s'est pas non plus prononcé de manière plus concrète à ce jour sur une éventuelle adaptation du seuil applicable aux dépôts du public dans le cadre de l'art. 1*b*, al. 2, de la LB. Il convient donc d'attendre un premier cas d'application de cette norme spéciale. 39

IV. CONDITIONS D'AUTORISATION (AL. 3 ET 4)

A. Champ d'activité (al. 3, let. a)

1. Généralités

Les statuts ou le **règlement d'organisation et de gestion** (ROG) doivent décrire avec précision le **champ d'activité** sur le plan matériel et géographique (art. 1*b*, al. 3, let. a, LB ; art. 14*b*, al. 1, OB). Le champ d'activité et son étendue géographique doivent correspondre aux capacités financières et à l'organisation administrative du requérant (art. 14*b*, al. 2, OB). Il est interdit aux établissements fintech de placer ou de rémunérer les dépôts du public ou les actifs cryptographiques qu'ils ont reçus (art. 1*b*, al. 1, let. b, LB). Il n'est pas 40

possible d'inscrire des activités dans les statuts ou dans le règlement d'exploitation «à titre préventif».

41 Les statuts ou le règlement d'exploitation doivent refléter de manière détaillée («précise») l'**activité actuelle** d'une personne au sens de l'art. 1*b* de la LB, tant sur le plan matériel, géographique que personnel. Les activités futures dépendent généralement de l'expérience acquise dans le cadre d'autres activités et doivent donc être précisées au moment de l'enregistrement et approuvées au préalable par la FINMA (cf. art. 8, al. 2, OB). À cet égard, une précision des dispositions correspondantes dans les statuts et le règlement interne est souvent exigée dans le cadre de la procédure d'autorisation.

42 La demande d'autorisation doit comporter les **informations générales** suivantes :

- motifs et objectif de l'obtention d'une autorisation en tant que personne au sens de l'art. 1*b* LB ;
- description détaillée de l'activité et de l'organisation prévues, y compris le champ d'activité matériel et géographique envisagé ainsi que le type de clientèle visé ;
- extrait du registre du commerce ;
- extrait du registre des poursuites (datant de moins de trois mois) de la requérante ;
- déclaration concernant les procédures en cours et clôturées (formulaire B1 ; signée et datée) de la requérante ;
- informations sur les sociétés du groupe ainsi que sur les participations et/ou autres implantations (succursales ou représentations) de la requérante.

43 Les informations requises concernant l'**activité commerciale, l'organisation et la gouvernance** de la requérante comprennent :

- une description détaillée des activités commerciales et des processus correspondants ;
- un plan d'affaires comprenant un budget (bilan, compte de résultat) pour les trois prochains exercices, avec des scénarios optimiste, réaliste et pessimiste ;

- une planification des liquidités pour le premier exercice selon le scénario pessimiste du plan d'affaires (sur une base mensuelle) ;
- les statuts, le règlement d'organisation et les directives (règlements et instructions) adaptés à l'activité commerciale d'une personne au sens de l'art. 1*b* de la LB ;
- un organigramme indiquant les noms des dirigeants et les ETP par unité organisationnelle ;
- Informations sur les locaux commerciaux (y compris la remise du contrat de location), l'infrastructure et les effectifs ;
- Organisation et règlements ou directives concernant la gestion des risques, la conformité et le système de contrôle interne (y compris les directives relatives à la LBA) ;
- Informations et documentation concernant l'externalisation d'activités (y compris l'analyse des risques, la directive relative aux objectifs, aux exigences, aux responsabilités et aux processus, l'inventaire des fonctions externalisées et les contrats d'externalisation) ;
- Informations et documentation concernant la gestion des risques opérationnels (notamment les risques liés aux technologies de l'information et de la communication (TIC), les cyber-risques, les risques liés aux données critiques, les risques liés à la conception et à la mise en œuvre de la gestion de la continuité des activités (BCM) et, le cas échéant, les risques liés aux activités de prestation de services transfrontalières), garantie de la résilience opérationnelle et rapports correspondants ;
- planification des TIC avec des précisions sur la capacité opérationnelle technique et opérationnelle des différentes applications et leur criticité ;
- vue d'ensemble de l'environnement TIC et applicatif envisagé ainsi que des interconnexions internes entre les systèmes (y compris les interfaces avec des systèmes tiers, les directives relatives aux systèmes TIC et à la sécurité des TIC, ainsi qu'au stockage et à la sécurité des données) lors du démarrage de l'activité opérationnelle ;
- Description de la manière dont les dépôts du public sont détenus (séparation par rapport aux fonds propres de l'entreprise) et de la manière dont le respect du seuil de 100 millions de CHF est garanti ;

- le cas échéant : description technique détaillée de la manière dont les actifs cryptographiques sont conservés ;
- informations détaillées sur les renseignements fournis aux clients conformément à l'art. 7*a* OB, notamment sur les risques ainsi que sur l'absence de garantie des dépôts.
- Description des éventuels conflits d'intérêts et des mesures prises à cet égard pour protéger les clients contre tout préjudice, conformément à l'art. 14*g* OB.

44 Les établissements titulaires d'une autorisation « fintech » peuvent en principe présenter des modèles d'affaires très variés (notamment le financement participatif, les opérations de paiement, que ce soit en utilisant des technologies traditionnelles ou des applications basées sur la technologie DLT/blockchain, etc.) . Dans la pratique, il s'est toutefois avéré jusqu'à présent que ce sont surtout les **prestataires de services de paiement** qui recourent à cette catégorie d'autorisation.

45 Outre les activités qui entraînent une obligation d'autorisation en tant qu'établissement fintech, celui-ci peut en principe également fournir des services accessoires qui, pris – considérés isolément – ne donneraient pas lieu à une obligation d'autorisation. La FINMA subordonne la fourniture d'un tel service accessoire, qui ne donnerait certes pas lieu en soi à une obligation d'autorisation mais qui accroît les risques de l'établissement, à la mise en œuvre de mesures appropriées d'atténuation des risques (cf. art. 14e, al. 1, OB). Si de telles mesures ne sont pas prises ou si les prescriptions relatives aux établissements fintech ne permettent pas de mettre en place des mesures adéquates de limitation des risques, la fourniture d'un service accessoire n'est pas compatible avec l'autorisation en tant qu'établissement fintech.

2. Conservation des dépôts du public et des actifs cryptographiques (al. 3, let. a)

a. Conservation des dépôts du public

46 Les établissements fintech doivent conserver les dépôts du public (au sens de l'art. 5 OB) et les actifs cryptographiques détenus en dépôt collectif (au sens de l'art. 5*a* OB) **séparément de leurs propres fonds** (art. 14*f* , al. 1, let. a, OB) . Dans ce cas, un contrôle restreint au sens de l'art. 727*a* du CO est

éventuellement possible (art. 14*f*, al. 1, let. b, OB *a contrario*) . Selon une interprétation littérale de l'art. 14*f* , al. 1, let. a, OB, il n'est pas admissible que des fonds de clients soient déposés sur un compte d'un prestataire de services tiers, par exemple un prestataire de services de paiement ne disposant pas d'une autorisation bancaire. Les dépôts éventuellement nécessaires auprès de tels prestataires de services de paiement devraient donc être préfinancés par les fonds de l'établissement fintech .

Une **exception** à cette séparation est accordée si les dépôts du public peuvent être comptabilisés à tout moment séparément des fonds propres et si un contrôle légal des comptes est effectué conformément à l'art. 727 CO (art. 14*f*, al. 1, let. b, OB). 47

Les entreprises sont toutefois tenues en premier lieu de transférer les fonds perçus conformément à l'accord conclu avec les clients ou, si tel n'est pas l'objectif ou si cela n'est pas possible, de les rembourser aux clients. Si un transfert immédiat n'est pas possible ou n'est pas prévu conformément à l'**accord avec le client**, l'entreprise est autorisée à conserver les dépôts. Cette « conservation » des dépôts n'est certes soumise à aucun délai, mais elle est soumise à certaines conditions : les dépôts doivent toujours être conservés dans l'intérêt des clients et ne doivent être ni placés ni rémunérés. Ils doivent être détenus soit sous forme de dépôts à vue auprès d'une banque, soit sous forme d'actifs hautement liquides. 48

Le **projet mis en consultation** du 21 juin 2018 ne contenait pas encore de let. b. La conservation séparée des dépôts du public reçus a constitué l'un des principaux points critiqués lors de la consultation, car elle aurait entraîné une charge organisationnelle et administrative considérable pour les établissements FinTech. En réponse à cette critique, le Conseil fédéral a prévu, à la let. b, la «séparation comptable» sous réserve d'un contrôle ordinaire au sens de l'art. 727 CO. 49

La détention des dépôts du public reçus est soumise à l'**interdiction légale de placement et de rémunération**. Cela signifie qu'ils doivent être détenus de manière à qui exclut dans une large mesure les risques pour les clients. Ils doivent en outre être disponibles sous forme de liquidités, de sorte qu'ils puissent être transférés conformément à leur destination ou remboursés dans un délai raisonnable. Une possibilité consiste notamment à déposer les fonds sous forme d'avoirs à vue sur un compte bancaire auprès d'une banque ou 50

d'une autre personne au sens de l'art. 1*b* LB. Il ne devrait pas y avoir de restrictions restrictives en matière de retrait.

51 Conformément au principe de séparation prévu à l'art. 14*f*, al. 1, let. a, OB, les dépôts du public peuvent être détenus sous forme de **dépôts à vue** auprès d'une banque ou d'un établissement de fintech et/ou sous forme d'**actifs liquides de haute qualité** (HQLA) de catégorie 1 au sens de l'art. 15*a* de l'ordonnance sur la liquidité du 30 novembre 2012 (OLiqu) (art. 14*f*, al. 2, OB). Les dépôts du public peuvent donc être détenus sous forme de pièces de monnaie, billets de banque ou sous forme d'avoirs auprès de la banque centrale, ou encore être investis dans certains titres négociables émis par des débiteurs spécifiques (tels que les gouvernements centraux), sans enfreindre l'interdiction de placement. Les établissements de monnaie électronique ne sont en principe pas reconnus dans ce contexte, sauf s'il existe une garantie des dépôts ou une sûreté similaire pour les fonds reçus.

52 Les dépôts du public doivent toujours être détenus dans la devise du **droit au remboursement** (art. 14*f*, al. 3, OB). Cela signifie notamment que les dépôts du public sous forme d'actifs cryptographiques détenus en dépôt collectif doivent être conservés en tant que tels (art. 14*f*, al. 4 OB). La possibilité de détenir des dépôts du public en HQLA permet, le cas échéant, aux établissements d'éviter les taux d'intérêt négatifs. Toutefois, cela engendre certains risques d'investissement pour les clients, ce qui peut entraîner des exigences plus élevées en matière de capital minimum.

53 Les clients ne doivent, dans la mesure du possible, être exposés à aucun risque supplémentaire, notamment **les risques de change**. C'est pourquoi les dépôts du public acceptés ne doivent être détenus que dans la devise dans laquelle un éventuel droit de remboursement existe.

54 Les dispositions relatives aux **dépôts privilégiés** (art. 37*a* LB) et au remboursement immédiat (art. 37*b* LB) ne s'**appliquent pas aux dépôts auprès des établissements fintech** (art. 1*b*, al. 4, let. d, LB), car le législateur estime actuellement qu'elles seraient disproportionnées. Par conséquent, les établissements fintech sont exemptés de l'obligation d'adhérer à l'autorégulation en matière de garantie des dépôts et des exigences de liquidité plus élevées applicables à la **garantie des dépôts**.

b. Surveillance du seuil applicable aux dépôts du public (al. 6)

55 La **limite** des dépôts du public et des jetons de paiement détenus en dépôt collectif à 100 millions de CHF est obligatoire (sous réserve de l'art. 1*b*, al. 2 et 5, LB). La demande d'autorisation doit décrire la manière dont le respect du seuil de 100 millions de CHF de dépôts du public est contrôlé. Les établissements fintech doivent donc disposer, en ce qui concerne la surveillance de ce seuil, de procédures documentées, de contrôles (responsabilité, périodicité), de rapports (y compris des prévisions) et d'autres mesures. À cet égard, un **système échelonné de mesures**, par exemple à 70, 80, 90 et 99 millions de CHF, peut s'avérer approprié. À partir d'un certain seuil, il convient en principe de prévoir des restrictions techniques afin qu'aucun nouveau dépôt du public ne soit plus accepté et que ceux-ci soient restitués. En outre, la coordination avec la FINMA doit être réglée.

57 Si plusieurs établissements fintech forment un **groupe financier** au sens de l'art. 22 OB, le seuil de 100 millions de CHF doit être calculé pour l'ensemble du groupe (art. 24*a*, al. 1, OB), sauf si les sociétés du groupe sont manifestement indépendantes les unes des autres. Cette mesure vise à empêcher que cette catégorie d'autorisation ne soit utilisée à des fins d'arbitrage réglementaire dans le domaine de l'acceptation de dépôts du public. Il s'agit donc d'empêcher la mise en place de montages visant à contourner le seuil de 100 millions de francs suisses.

3. Conservation des actifs cryptographiques

58 Les **actifs cryptographiques** conservés en dépôt collectif doivent être détenus en Suisse et sous la forme sous laquelle ils ont été acceptés (art. 14*f*, al. 4, OB) . Le pouvoir de disposition sur les clés privées appartient donc en principe de manière impérative et exclusive aux établissements fintech ou aux banques domiciliés en Suisse. Les établissements fintech définissent, dans des directives internes, la gestion des clés cryptographiques permettant l'accès aux actifs cryptographiques. Ces directives internes doivent notamment a. régir la gestion et le contrôle de toutes les clés nécessaires, c'est-à-dire leur conservation sécurisée, leur mise à disposition, leur transmission sécurisée ainsi que le retrait des clés cryptographiques invalides ou compromises.

59 Les **clés cryptographiques** peuvent, par exemple, être stockées dans un module de sécurité matériel (HSM). En ce qui concerne la sécurité des HSM,

l'établissement fintech doit s'aligner sur la norme FIPS (FIPS) 140 du gouvernement américain. Cette norme définit les exigences minimales de sécurité pour les modules cryptographiques intégrés aux produits informatiques et est inscrite dans la section 5131 de l'Information Technology Management Reform Act de 1996.

60 D'une manière générale, il convient de s'assurer que l'accès aux actifs cryptographiques ne soit possible qu'au moyen d'une **procédure de signature multi** . L'une des clés partielles doit être gérée par un membre de la direction. L'utilisation d'une clé privée doit impérativement être précédée de l'identification de l'ayant droit. Pour les transactions dépassant un certain montant, l'accord d'un deuxième membre de la direction doit être obtenu. Pour la signature de transactions d'un montant négligeable, une procédure simplifiée de gestion des clés peut être prévue. L'utilisation de clés privées pour la signature de transactions est soumise à des exigences de documentation, dont le respect doit être régulièrement vérifié dans le cadre du système de contrôle interne (SCI).

61 Les établissements fintech doivent en outre s'assurer qu'en cas de perte de clés partielles (p. ex. à la suite d'un incendie ou d'un événement similaire), l'accès aux actifs cryptographiques soit possible via une **clé de sauvegarde/ récupération/clé principale** (*seed*). Cette clé doit être conservée dans un lieu distinct de celui où sont conservées les autres clés privées (p. ex. dans un coffre-fort chez un prestataire de services financiers) . L'accès et l'échange doivent être régis par une directive interne.

62 La FINMA peut, au cas par cas, fixer un **plafond** pour les actifs cryptographiques si cela semble justifié au vu des risques liés à l'activité. L'autorité de surveillance tient notamment compte de la fonction des actifs cryptographiques, des technologies sous-jacentes ainsi que des facteurs atténuant les risques (art. 4^{sexies} LB).

63 Les établissements proposant la conservation d'actifs cryptographiques doivent établir un *Digital Asset Resolution Package* (DARP). L'objectif de ce document est de garantir qu'en cas de faillite de l'établissement, un liquidateur externe puisse rapidement reverser les actifs cryptographiques aux clients, de manière à minimiser les efforts et les coûts liés à une restitution en bonne et due forme. À cette fin, le DARP doit contenir les informations essentielles permettant l'identification et la sécurisation rapide des actifs

cryptographiques, telles que des indications sur toutes les personnes nécessaires à la conservation et aux opérations des actifs cryptographiques, y compris les instructions associées, les informations permettant d'accéder à une copie à jour du registre interne (Internal Ledger), y compris les instructions associées, les informations concernant d'éventuels dépositaires tiers, y compris les coordonnées des personnes responsables de la banque auprès du dépositaire tiers, etc. Il convient de veiller à ce que l'établissement mette régulièrement à jour le DARP.

B. Organisation administrative appropriée (al. 3, let. a)

Les établissements Fintech doivent disposer d'une **organisation administrative** adaptée à leur activité (champ d'activité et étendue géographique de celle-ci) (art. 1*b*, al. 3, let. a, LB ; art. 14*b*, al. 2, OB). 64

1. Forme juridique, siège et lieu d'activité

Les établissements fintech revêtent la **forme juridique** d'une société anonyme, d'une société en commandite par actions ou d'une société à responsabilité limitée et ont leur siège en Suisse (art. 14*a* OB). Cette exigence vise à garantir une surveillance adéquate. 65

D'un point de vue dogmatique, le renvoi général par analogie de l'art. 1*b*, al. 1, LB peut être interprété en ce sens que la **coopérative** devrait être reconnue comme une forme juridique admissible, contrairement au libellé de l'ordonnance. Toutefois, en raison des difficultés liées au capital social devant être maintenu en permanence, aux règles d'organisation et de prise de décision lourdes (notamment le droit de vote par tête) ainsi que des parts sociales, qui ne peuvent être titrisées en tant que valeurs mobilières, cette forme juridique n'est toutefois pas adaptée à l'exploitation d'un établissement fintech. 66

L'activité principale ou la gestion effective doit être exercée en **Suisse** et l'établissement de fintech doit être effectivement dirigé depuis la Suisse. Les personnes chargées de la direction doivent être domiciliées dans un lieu à partir duquel elles peuvent effectivement exercer la direction (art. 14*a*, al. 2, et art. 14*c* OB). 67

Les personnes chargées de la **direction** doivent avoir leur domicile à proximité du siège de la requérante. Il est exigé qu'elles aient leur domicile à 68

proximité ou en Suisse. Conformément à la pratique actuelle de la FINMA, on attend donc qu'au moins une partie des personnes chargées de la direction soit présente au siège chaque jour ouvrable. Cette mesure vise à garantir qu'un établissement fintech suisse ne soit pas, dans les faits, dirigé depuis l'étranger.

69 Conformément à la pratique de surveillance actuelle, il convient, dans le cas des garants titulaires d'un permis de séjour de courte durée à durée déterminée (titre L), le risque d'extinction des **droits de séjour** doit être pris en compte de manière appropriée. L'établissement doit recenser ce risque dans le cadre de sa gestion des risques et le couvrir par des mesures appropriées, notamment des procédures de notification, de suppléance et de succession.

70 En ce qui concerne la **raison sociale**, l'art. 1, al. 4, de la LB stipule que les termes «banque» ou «banquier», seuls ou dans des combinaisons de mots, dans la raison sociale, dans la désignation de l'objet social et dans la publicité commerciale, ne peut être utilisé, dans l'intérêt de la protection des créanciers, que pour les établissements disposant d'une autorisation de la FINMA en tant que banque ; sont également concernés les termes équivalents dans toutes les langues nationales et toutes les langues étrangères, ainsi qu'en principe les combinaisons de mots suggérant une activité bancaire, sont également incluses. Les combinaisons de mots comportant les éléments «*bank*» ou «*banking*» sont donc à considérer avec prudence (y compris sur le site web, dans le registre du commerce ou dans les statuts). Cela inclut même des variantes plus créatives telles que «*non-bank*» ou «*neo-bank*». En revanche, des termes tels que «*money accounts*», «*payment accounts*», «*payment services*» ou des combinaisons de mots similaires ne devraient pas poser de problème, car les services de paiement ne doivent pas nécessairement être fournis par une banque ; une affiliation à un OAR peut déjà suffire.

71 En application par analogie de l'art. 4*quater* LB aux établissements fintech, ceux-ci doivent donc s'abstenir, tant en Suisse qu'à l'étranger, de toute **publicité** trompeuse ou intrusive faisant référence à leur siège social en Suisse ou aux dispositifs suisses de protection des créanciers.

2. Organes

Si l'objet social ou l'étendue des activités d'un établissement fintech nécessite un organe spécifique chargé de la haute direction, de la surveillance et du contrôle, celui-ci doit être composé d'au moins trois membres (art. 14*d*, al. 1, OB) . Les établissements fintech doivent en règle générale disposer d'**organes d'administration et de direction**, l'organe chargé de la haute direction, de la surveillance et du contrôle (conseil d'administration) devant compter au moins trois membres. Au moins un tiers des membres du conseil d'administration doit être indépendant de la direction (art. 14*d*, al. 2, OB). 72

Un membre de l'organe de direction générale est considéré comme **indépendant** s'il : 73

- n'est pas employé par l'établissement à un autre titre et ne l'a pas été au cours des deux dernières années ;
- n'a pas été employé, au cours des deux dernières années, par la société d'audit de l'établissement en tant qu'auditeur responsable de celui-ci ;
- n'entretient aucune relation d'affaires avec l'établissement qui, de par sa nature ou son ampleur, conduirait à un conflit d'intérêts ;
- n'est pas une personne concernée non qualifiée (au sens de l'art. 3, al. 2, let. c^{bis}, LB) de l'établissement et n'en représente pas non plus ; et
- n'entretient en principe aucune relation de proximité (parenté, mariage ou union libre) avec un membre de la direction.

Dans des cas justifiés, la FINMA peut accorder des **dérogations** aux exigences applicables aux organes (art. 14*d*, al. 4, OB). La séparation des pouvoirs et des fonctions n'est donc pas absolue. Ainsi, la FINMA peut par exemple autoriser un établissement fintech à ne disposer que d'une direction, mais pas d'un conseil d'administration. Cette dérogation est destinée aux très petits établissements en phase de démarrage. Il est notamment envisageable que des *start-ups* se voient accorder temporairement des dérogations aux exigences relatives à l'organisation administrative jusqu'à ce qu'elles atteignent certains objectifs de croissance ; par exemple, des membres indépendants du conseil d'administration (et des fonctions de contrôle indépendantes) ne seraient requis qu'à partir d'un produit brut de 1 million de CHF (et à partir de 1,5 million de CHF). 74

75 La notion d'organe se rapporte aux **personnes physiques**. Les personnes morales ne sont donc pas considérées comme des organes. La FINMA vérifie, pour les membres du conseil d'administration et de la direction, ce qu'on appelle la **garantie d'une activité irréprochable**. Cet examen est, par nature, axé sur la personne et présuppose l'évaluation de l'intégrité, de la réputation personnelle, des qualifications professionnelles, de l'expérience et des conflits d'intérêts.

76 Les **pièces justificatives** requises concernant les organes comprennent :

- la composition de l'organe chargé de l'administration, avec indication du président, du vice-président ainsi que des membres d'éventuels comités ; ainsi que
- des informations sur la composition, l'organisation et les compétences de la direction.

3. Infrastructure et personnel

ux a. Locaux commercia

77 La requérante doit disposer de **locaux commerciaux adaptés**. En ce qui concerne la taille, un bureau et une salle de réunion peuvent suffire. Si elle ne dispose pas de biens immobiliers, elle doit présenter un contrat de (sous-)location doit être présenté. Des informations sont requises concernant les possibilités d'accès et les restrictions d'accès, la possibilité de fermer à clé les locaux et le mobilier, ainsi que la conduite des activités quotidiennes dans le respect du secret des données et du secret bancaire (par exemple, un accord de confidentialité garantissant le respect des règles de confidentialité applicables à la requérante dans le cadre de ses activités quotidiennes [notamment en matière de circulation des personnes, de courrier et d'infrastructure TIC physique]). Il est en outre nécessaire que la direction opérationnelle effective de la société s'exerce à partir des locaux commerciaux concernés.

b. Ressources humaines

78 En ce qui concerne les ressources humaines, il est essentiel que l'établissement fintech ait pourvu les postes nécessaires et soit en mesure de réagir rapidement si du **personnel** supplémentaire s'avère nécessaire pour

l'activité commerciale. À cette fin, des informations correspondantes doivent être fournies et les équivalents temps plein (ETP) pourvus, y compris les domaines d'activité, doivent idéalement être présentés à l'aide d'un graphique.

c. Infrastructure technique

En règle générale, les établissements fintech ne disposent pas de leur propre infrastructure TIC physique, à l'exception des terminaux ainsi que des infrastructures d'alimentation électrique, de téléphonie et de connexion Internet. La majeure partie de l'**infrastructure TIC** est souvent basée sur le cloud, ce qui comporte généralement des risques. 79

Dans le cadre de la demande, une présentation plus détaillée de l'architecture TIC prévue et des composants TIC nécessaires aux activités prévues est requise. En conséquence, un plan TIC comprenant des informations sur la **capacité opérationnelle** technique et opérationnelle des différentes applications ainsi que sur leur criticité est également nécessaire. L'établissement fintech doit fournir des informations à cet égard concernant la capacité opérationnelle et technique de ses applications TIC. Il doit présenter, dans un calendrier, l'état d'avancement ainsi que la mise en œuvre des applications qu'il prévoit de déployer et se prononcer sur leur criticité en vue de leur mise en service. 80

4. Externalisation

a. Possibilité d'externalisation

Les établissements fintech sont en principe autorisés à externaliser des fonctions et des activités (principe de l'externalisation). L'**externalisation** de fonctions essentielles est donc autorisée. Les exigences de la circulaire FINMA 2018/3 « Externalisation » s'appliquent aux établissements fintech dans une mesure adaptée. Ces exigences doivent être mises en œuvre en tenant compte de la taille, de la complexité, de la structure et du profil de risque de l'établissement. 81

Afin de garantir la visibilité et le contrôle, les fonctions essentielles externalisées et les prestataires de services correspondants doivent être répertoriés dans l'**OGR**. 82

83 Les entreprises des catégories de surveillance 1 à 3 disposent d'une fonction autonome de contrôle des risques et de conformité, agissant en tant qu'instances de contrôle indépendantes. Pour les **établissements fintech**, il suffit qu'une personne responsable de ces fonctions soit désignée au sein de la direction. Les tâches opérationnelles de gestion des risques et de conformité peuvent être externalisées dans toutes les catégories de surveillance.

84 **Ne peuvent pas être externalisés** : la haute direction, la surveillance et le contrôle par le conseil d'administration, les tâches de direction centrales de la direction générale ainsi que les fonctions impliquant des décisions stratégiques. Cela vaut également pour les décisions relatives à l'établissement et à la résiliation de relations d'affaires.

b. Caractère significatif

85 La qualification d'une externalisation comme significative ou non significative peut soulever des questions. En outre, il convient de distinguer les externalisations des coopérations avec des prestataires tiers, qui fournissent des prestations ne faisant pas partie intégrante de l'activité commerciale ou des fonctions opérationnelles de l'établissement de fintech vis-à-vis de ses clients, par exemple des relations d'affaires directes avec l'établissement de fintech ou avec les clients de celui-ci. Dans ce dernier cas, l'établissement de fintech n'intervient pas en tant que partie contractante, mais en tant qu'intermédiaire. Le **caractère significatif** doit généralement être retenu, lorsque le prestataire a accès à des données critiques de l'entité soumise à surveillance et qu'il pourrait extraire, voire manipuler, ces données. Le caractère essentiel d'une externalisation est également avéré lorsqu'une défaillance du prestataire affecte directement l'activité opérationnelle de l'entité soumise à surveillance. De plus en plus de fonctions ont tendance à être considérées comme essentielles en raison de leur dépendance opérationnelle directe.

86 En règle générale, dans le cadre de l'activité des établissements fintech, il convient de considérer qu'il s'agit d'une **externalisation essentielle** pour les services et fonctions suivants :

- services logiciels et de serveurs allant au-delà d'une simple assistance, dans la mesure où ils influencent directement l'activité opérationnelle ;

- système bancaire central (dans la mesure où il existe une dépendance directe et urgente) ;
- infrastructure informatique basée sur le cloud ;
- solutions SaaS, dans la mesure où l'exploitation est assurée par le prestataire et qu'il en résulte une dépendance directe pour l'activité opérationnelle) ;
- passerelle SIC ;
- sponsor BIN/SIC (par opposition aux émetteurs de cartes) ;
- prestataires de transactions en devises étrangères, dans la mesure où l'intégration des services va bien au-delà de la relation traditionnelle de correspondance bancaire ;
- prestataires de services de change, dans la mesure où le processus est essentiel à la prestation de services de l'établissement fintech ;
- toutes les fonctions et instances de contrôle : contrôle des risques, fonction de conformité, service spécialisé dans la lutte contre le blanchiment d'argent, audit interne ;
- systèmes KYC (identification et vérification lors de l'accès à des données critiques) ;
- Identification à deux facteurs ;
- Surveillance des transactions ;
- Fonction de délégué ou de conseiller à la protection des données.

Ne sont généralement pas considérés comme essentiels les services et fonctions externalisés suivants : 87

- Services de vérification (d'adresses de domicile ou de numéros de téléphone portable) ;
- la mise à disposition d'infrastructures de base (par exemple, Internet) et de bases de données (par exemple, listes de sanctions pour le KYC) ;
- services administratifs classiques (tels que le conseil juridique, le conseil économique, la comptabilité, la présentation des comptes, le conseil fiscal, la gestion des ressources humaines, les relations publiques et la communication, ainsi que le marketing), car ceux-ci sont plus faciles à remplacer et ne créent en principe aucune dépendance.

c. Inventaire

88 Les établissements fintech doivent tenir un **inventaire** à jour des fonctions externalisées. Celui-ci contient une description de la fonction externalisée, mentionne les prestataires (y compris les sous-traitants) et les bénéficiaires des prestations, ainsi que le service responsable au sein de l'entreprise.

d. Analyse des risques

89 Dans le cadre de l'externalisation, la requérante doit établir une **analyse des risques** qui englobe les considérations économiques et opérationnelles essentielles ainsi que les risques et opportunités qui y sont liés. Si plusieurs fonctions sont externalisées auprès du même prestataire, il convient de tenir compte du risque de concentration.

e. Sélection, instruction et contrôle du prestataire

90 Lors de la **sélection** du prestataire, il convient de prendre en compte et de vérifier ses compétences techniques ainsi que ses ressources financières et humaines. Lors de la décision d'externalisation et de la sélection du prestataire, il faut également tenir compte des possibilités et des conséquences d'un changement de prestataire. Le prestataire doit garantir la continuité de la prestation.

91 Dans le cadre des **instructions**, les compétences de l'entreprise et du prestataire doivent être définies et délimitées contractuellement, notamment en ce qui concerne les interfaces et les responsabilités.

92 La fonction externalisée doit être intégrée dans le **SCI** de l'entreprise. Les risques significatifs liés à l'externalisation doivent être systématiquement identifiés, surveillés, quantifiés et maîtrisés. Au sein de l'entreprise, il convient de désigner un service responsable chargé de la surveillance et du pilotage du prestataire. Les prestations du prestataire doivent faire l'objet d'une surveillance et d'une évaluation continues afin que les mesures nécessaires puissent être prises en temps utile, le cas échéant.

f. Audit et surveillance

93 L'entreprise, sa société d'audit ainsi que la FINMA doivent être en mesure de vérifier le respect des dispositions réglementaires par le prestataire de services. Un **droit de consultation et de contrôle** à tout moment, illimité et

sans entrave concernant la fonction externalisée doit leur être accordé contractuellement.

Les activités d'audit peuvent être déléguées à l'organe de révision du prestataire de services, pour autant que celui-ci dispose de la compétence technique nécessaire. En cas d'une telle **délégation**, la société d'audit de l'entreprise peut s'appuyer sur les résultats d'audit de l'organe de révision du prestataire de services. 94

L'externalisation d'une fonction ne doit pas entraver la **surveillance** exercée par la FINMA, en particulier en cas d'externalisation à l'étranger. 95

Si le prestataire de services n'est pas soumis à la surveillance de la FINMA, il doit s'engager contractuellement envers la requérante à fournir à la FINMA toutes les **renseignements et documents** relatifs au domaine d'activité externalisé dont elle a besoin pour exercer son activité de surveillance. Si des activités d'audit sont déléguées à l'organe de révision du prestataire de services, son rapport doit être mis à la disposition de la FINMA, de l'organe de révision interne et de la société d'audit de l'entreprise qui externalise ces activités, sur simple demande. 96

g. Contrats d'externalisation

Conformément aux objectifs poursuivis par l'externalisation, les exigences relatives à la prestation de services doivent être définies et documentées avant la conclusion du contrat. Cela inclut une **analyse des risques** qui englobe les principales considérations économiques et opérationnelles ainsi que les risques et opportunités qui y sont liés. 97

Les **compétences** du requérant et du prestataire de services doivent être définies et délimitées contractuellement, notamment en ce qui concerne les interfaces et les responsabilités. 98

Le requérant doit se faire accorder contractuellement par le prestataire de services les **droits d'instruction et de contrôle** nécessaires à la surveillance et au contrôle de ce dernier par le prestataire de services. En cas d'externalisation ayant une incidence sur la sécurité (notamment dans le domaine informatique), l'entreprise et le prestataire de services définissent contractuellement des exigences de sécurité. Leur respect doit être surveillé par l'institut fintech. 99

100 Afin de vérifier le respect des dispositions prudentielles par le prestataire de services, un **droit de consultation et de contrôle** à tout moment, complet et sans entrave doit être accordé contractuellement en ce qui concerne la fonction externalisée.

101 Si le prestataire de services (étranger) n'est pas soumis à la surveillance de la FINMA, il doit s'engager contractuellement envers l'entreprise à mettre à la disposition de la FINMA toutes les **informations et tous les documents** nécessaires à l'exercice de sa surveillance concernant le domaine d'activité externalisé.

102 L'externalisation doit reposer sur un contrat **écrit** ou sur un contrat sous une autre forme permettant d'en conserver une trace écrite. Outre la désignation des parties et la description des fonctions, celui-ci doit contenir au moins les éléments prévus dans la circulaire FINMA 2018/3.

103 L'établissement veille à être informé en temps utile du recours à des sous-traitants ou d'un **changement** de ceux-ci lorsqu'ils exercent des fonctions essentielles. Si de tels sous-traitants sont engagés, il convient de leur imposer les obligations et les garanties du prestataire de services nécessaires au respect de la circulaire FINMA 2018/3. La possibilité de faire appel à des sous-traitants doit en outre être régie dans le règlement d'organisation et de gestion (ROG).

104 De manière générale, des dispositions contractuelles doivent être prises pour mettre en œuvre les **exigences** de la circulaire FINMA 2018/3.

105 L'établissement doit définir les procédures internes d'autorisation pour les **projets d'externalisation** ainsi que les compétences en matière de conclusion des contrats correspondants.

h. Rapports

106 La mise en œuvre de la surveillance et du contrôle requis du prestataire de services peut, dans le cas des établissements fintech par le biais de **rapports** réguliers établis par un organe de révision indépendant, compte tenu de la possibilité de déléguer les activités de contrôle à l'organe de révision du prestataire de services. Ces rapports doivent permettre d'évaluer les risques significatifs liés à l'externalisation ainsi que les activités de contrôle du prestataire de services.

i. Situations au sein du groupe

En ce qui concerne les exigences relatives à la sélection, à l'instruction et au contrôle du prestataire ainsi qu'aux conditions contractuelles, l'appartenance au groupe peut être prise en compte, pour autant qu'il soit démontré que les risques typiquement liés à l'externalisation n'existent pas ou que certaines exigences ne sont pas pertinentes ou font l'objet d'une réglementation différente. 107

j. Responsabilité et sécurité

L'établissement fintech reste **B responsable**B vis-à-vis de la FINMA, comme s'il exerçait lui-même la fonction externalisée. Il doit garantir à tout moment une gestion conforme. 108

En cas d'externalisation ayant une incidence sur la sécurité (notamment dans le domaine informatique), l'établissement et le prestataire de services définissent des **exigences de sécurité** contractuelles. Le respect de celles-ci doit être contrôlé par l'entreprise. 109

Dans ce cadre, l'établissement et le prestataire de services élaborent un **dispositif de sécurité** permettant la poursuite de la fonction externalisée en cas d'urgence. Lors de la mise en place et de l'application du dispositif de sécurité, l'entreprise applique le même niveau de diligence que si elle assurait elle-même la fonction externalisée. 110

k. Externalisation à l'étranger

L'externalisation à l'**étranger** est autorisée pour autant que l'établissement puisse garantir expressément que lui-même, sa société d'audit ainsi que la FINMA puissent exercer et faire valoir leurs droits de consultation et de contrôle. La possibilité d'assainissement ou de liquidation de l'établissement en Suisse doit en outre être garantie. L'accès aux informations nécessaires à cet effet doit enfin être possible à tout moment en Suisse. 111

l. Conditions et exceptions

La FINMA peut, dans des cas justifiés, imposer des **conditions** à l'établissement fintech ou le dispenser, en tout ou en partie, du respect de la circulaire FINMA 2018/3. 112

11 3 Les établissements évaluent et décident de la pertinence et de la mise en œuvre des exigences relatives au choix du prestataire de services dans le cadre de leur **analyse des risques**.

11 4 Les établissements fintech sont exemptés de l'exigence d'une réintégration ordonnée de la fonction externalisée. L'intégration de la fonction externalisée dans le système de contrôle interne peut, pour les établissements fintech, s'effectuer par le biais de **rapports** réguliers établis par un organe de révision indépendant. Ces rapports doivent permettre d'évaluer les risques significatifs liés à l'externalisation ainsi que les activités de contrôle du prestataire de services.

C. Gouvernance d'entreprise : gestion des risques, contrôles internes et conformité (al. 3, let. b)

1. Principes fondamentaux

11 5 Les établissements fintech doivent disposer d'un **système de gestion des risques** doté de ressources adéquates et d'un **SCI efficace**, garantissant notamment le respect des prescriptions légales et internes à l'entreprise (**conformité**) (art. 1*b*, al. 3, let. b, LB et art. 14*e*, al. 1, OB).

11 6 La **gestion des risques** englobe les structures organisationnelles ainsi que les méthodes et processus qui servent à définir des stratégies de gestion des risques et des mesures de maîtrise des risques, ainsi qu'à identifier, analyser, évaluer, gérer, surveillance et au reporting des risques.

11 7 Le **SCI** englobe l'ensemble des structures et processus de contrôle qui, à tous les niveaux de l'établissement, constituent la base permettant d'atteindre les objectifs de la politique d'entreprise et d'assurer le bon fonctionnement de l'établissement. À cet égard, le SCI ne comprend pas seulement des activités de contrôle a posteriori, mais aussi des activités de planification et de pilotage. Le SCI met l'accent sur la réalisation des objectifs de l'entreprise, la protection de ses actifs, la garantie de la sécurité des processus ainsi que la prévention ou la détection d'irrégularités. Un SCI efficace comprend notamment des activités de contrôle intégrées dans les processus opérationnels, des processus appropriés de gestion des risques et de conformité, ainsi que des instances de contrôle adaptées à la taille,

complexité et au profil de risque de l'établissement, notamment une fonction indépendante de contrôle des risques et de conformité.

Parmi les exemples de risques potentiels figurent les dysfonctionnements internes des technologies de l'information et de la communication (TIC), les difficultés liées aux fonctions externes, les pandémies, la perte de personnel essentiel ou de clients clés, les problèmes de liquidités, les risques juridiques, les cyberattaques, les pannes de système, les défaillances des chaînes d'approvisionnement, les coupures d'électricité à grande échelle ou prolongées, les catastrophes naturelles, la perte de données, la dépendance vis-à-vis de prestataires tiers, les atteintes à la réputation, les nouvelles dispositions réglementaires, les risques liés au blanchiment d'argent, le terrorisme, la fraude, les retards dans les infrastructures de paiement ou les risques de change. 11 8

On entend par **conformité** le respect des dispositions légales, réglementaires et internes, ainsi que le respect des normes en vigueur sur le marché et des règles déontologiques. 11 9

Les établissements fintech veillent donc à une identification, une évaluation, une gestion et une surveillance efficaces des risques liés à leur activité, ainsi qu'à la mise en place d'un système de contrôle interne efficace (art. 14*e*, al. 1, OB) . La manière dont les exigences susmentionnées sont satisfaites doit être consignée dans la **documentation interne et les directives** (art. 14*e*, al. 2, OB). 12 0

Le **secret bancaire** s'applique également aux organes, aux employés, aux mandataires ou aux liquidateurs des établissements fintech (art. 47, al. 1, let. a, LB). 12 1

La circulaire FINMA 2017/1 «Gouvernance d'entreprise – Banques» ne s'applique **pas** aux établissements fintech, ce qui est approprié, car cela ne serait pas pertinent au regard du principe de proportionnalité qui y est énoncé. En matière de gouvernance d'entreprise, ce sont donc les dispositions de la LB, de l'OB et du CO (ainsi que, à titre d'autorégulation, le « Swiss Code of Best Practice for Corporate Governance ») qui s'appliquent. La circulaire FINMA 2017/1 peut toutefois servir d'aide à l'interprétation en ce qui concerne la terminologie. 12 2

12 La **circulaire FINMA 2023/01** « Risques opérationnels et résilience –
3 Banques » s'applique en revanche directement aux établissements de fintech, certaines dispositions ne s'appliquant toutefois pas à ces derniers.

2. Fonctions de contrôle indépendantes

12 Les services chargés de la **surveillance** de la conformité et de la gestion des
4 risques doivent être indépendants, en interne, des activités à but lucratif (art. 14*e*, al. 3, OB). La FINMA peut, au cas par cas, accorder des dérogations à ces exigences si l'établissement de fintech : a) réalise un produit brut inférieur à 1,5 million de CHF ; ou b) apporte la preuve qu'il dispose d'un modèle d'affaires à faible risque (art. 14*e*, al. 5, OB).

12 L'établissement fintech peut faire appel à des **tiers** pour la surveillance de la
5 conformité et la gestion des risques, pour autant que ceux-ci disposent des compétences, des connaissances et de l'expérience requises pour cette activité, ainsi que des autorisations éventuellement nécessaires. Il forme et supervise avec soin les tiers auxquels il fait appel (art. 14*e*, al. 4, OB).

12 Les établissements fintech mettent généralement en place deux instances de
6 contrôle interne ou **lignes de défense** : au premier niveau, les unités opérationnelles axées sur le résultat assurent la gestion des risques, notamment par leur surveillance, leur pilotage et leur reporting directs, et garantissent le respect des exigences légales dans le cadre de leurs activités quotidiennes (*première ligne de défense*). Au deuxième niveau (*deuxième ligne de défense*), les fonctions de contrôle des risques et de conformité surveillent les risques ainsi que le respect des prescriptions légales, réglementaires et internes. Au troisième niveau, enfin, un contrôle peut être effectué, le cas échéant, par un service d'audit interne (*troisième ligne de défense*). La question de savoir si et dans quelle mesure un établissement de fintech doit garantir ces trois niveaux dépend essentiellement du cas concret.

12 En règle générale, seules une **deuxième ligne de défense**, à savoir le
7 contrôle des risques et la fonction de conformité, est requise. Les services chargés du contrôle des risques et de la conformité doivent être indépendants des activités à but lucratif. Il convient d'examiner au cas par cas si la disposition dérogatoire de l'art. 14*e*, al. 4, OB s'applique. Lors de l'évaluation au cas par cas, il faut notamment tenir compte du risque de conflits d'intérêts. Si des conflits d'intérêts ne peuvent être exclus, une fonction indépendante de

gestion des risques et de conformité doit dans tous les cas être mise en place. Il convient en outre de prendre en compte les compétences et les connaissances des personnes impliquées ainsi que toute activité commerciale éventuelle déjà exercée.

La LB et, en particulier, l'art. 14*e* de l'Ordonnance sur les banques (OB) ne mentionnent pas l'audit interne comme un élément (vraisemblablement obligatoire) du SCI pour les établissements fintech. Un **audit interne** n'est donc pas obligatoire pour les établissements fintech. La nécessité d'en disposer dépend essentiellement, au regard des risques, du cas concret, c'est-à-dire de la taille, de l'activité commerciale et de l'organisation en place. En règle générale, il est possible de se passer d'un service d'audit interne. 128

3. Gestion des risques

a. Responsabilités

La gestion des **risques opérationnels** s'inscrit dans le cadre de la gestion des risques à l'échelle de l'établissement. La politique de gestion des risques et les grandes lignes de la gestion des risques régissent la gestion des risques significatifs, la tolérance au risque et les limites de risque qui en découlent dans toutes les catégories de risques significatives. 129

L'**organe de direction** approuve les principes fondamentaux de la gestion des risques opérationnels pertinents pour l'établissement et veille à leur respect. Il approuve au moins une fois par an la tolérance au risque opérationnel, conformément à la politique de risque et en tenant compte des objectifs stratégiques et financiers de l'établissement. Ce faisant, il tient compte des résultats des évaluations des risques et des contrôles. Il accepte soit le niveau d'exposition de l'établissement aux risques opérationnels, soit décide d'un ajustement de la tolérance au risque et des changements stratégiques nécessaires à cet effet, tels qu'une modification du modèle économique. 130

Dans ce cadre, l'organe de direction approuve régulièrement **des stratégies** documentées relatives à la gestion des TIC, des cyber-risques, des données critiques et de la gestion de la continuité des activités (BCM), et veille à leur respect. 131

13 2 La **direction** veille, de manière vérifiable, à ce que les risques opérationnels soient identifiés, évalués, limités et surveillés, et à ce que tant la conception que la mise en œuvre de cette gestion des risques opérationnels fassent l'objet d'un contrôle régulier de leur efficacité. Afin de limiter les risques inhérents jugés significatifs (dits « risques majeurs » ou « risques clés »), elle prend, en fonction de la situation, des mesures complémentaires ou renforcées spécifiques aux risques.

13 3 Si nécessaire, la **FINMA** définit, dans le cadre de la surveillance courante, des exigences supplémentaires en matière de gestion des risques opérationnels pour des thèmes spécifiques. Cela s'effectue selon le principe de proportionnalité.

b. Inventaire

13 4 Les risques opérationnels doivent être classés de manière uniforme à l'échelle de l'établissement et consignés dans un **inventaire**. La classification peut s'appuyer sur celle des types d'événements utilisée pour le calcul de l'exigence minimale de fonds propres pour les risques opérationnels ou s'appuyer sur une taxonomie interne. La classification doit être appliquée de manière cohérente dans tous les domaines de l'établissement et dans toutes les composantes de la gestion des risques opérationnels.

c. Identification

13 5 Les **risques opérationnels** comprennent notamment les risques liés aux TIC, les cyber-risques, les risques liés aux données critiques, les risques découlant de la conception et de la mise en œuvre de la gestion de la continuité des activités (BCM) ainsi que, le cas échéant, les risques liés aux activités de prestation de services transfrontalières. Pour la définition, il est possible de se référer à la définition légale figurant à l'article 89 de l'ordonnance sur les fonds propres (OFR), selon laquelle on entend par risques opérationnels le risque de pertes résultant de l'inadéquation ou de la défaillance de procédures internes, de personnes et de systèmes, ou d'événements externes. Sont inclus les risques juridiques, mais non les risques stratégiques ni les risques de réputation.

13 6 Lors de l'**identification** des risques opérationnels, il convient de prendre en compte tant les facteurs internes qu'externes. Les risques opérationnels identifiés doivent faire l'objet d'une évaluation compréhensible tant sous

l'angle des risques inhérents que sous celui des risques résiduels. Parmi les facteurs internes figurent par exemple les changements au niveau des produits, des activités, processus et systèmes, ainsi que les résultats d'audit et les pertes internes liées aux risques opérationnels. Les facteurs externes comprennent, par exemple, les événements ayant entraîné des pertes identifiés chez d'autres établissements, les changements de la situation en matière de sécurité (par exemple dus à des influences environnementales, à des cyberattaques ou au terrorisme) ou les modifications des exigences réglementaires.

L'identification et l'évaluation des risques opérationnels doivent s'appuyer au minimum sur les **résultats d'audit** et sur des évaluations régulières des risques et des contrôles. Les résultats d'audit devraient (dans la mesure où ils sont disponibles) inclure les résultats de l'audit interne et de la société d'audit externe, ainsi que les résultats des vérifications effectuées, par exemple, par les divisions opérationnelles et organisationnelles, le contrôle des risques, la fonction de conformité ou les autorités de surveillance. 137

d. Tolérance au risque

La **tolérance au risque** pour les risques opérationnels tient compte à la fois de la tolérance vis-à-vis des risques opérationnels inhérents et résiduels et est surveillée à l'aide d'indicateurs de risque ou de contrôle. 138

La tolérance au risque relative aux **risques inhérents** tient compte des décisions stratégiques concernant le modèle d'affaires ou d'exploitation, par exemple la tolérance vis-à-vis des risques inhérents liés au service de certains segments de clientèle ou de certains pays, à l'offre de certains produits, à l'utilisation de processus essentiellement manuels, à la dépendance à l'égard d'une infrastructure informatique complexe ou à certaines externalisations. 139

e. Formation du personnel

Des mesures visant à **sensibiliser** le personnel à la réduction des risques opérationnels pertinents, en particulier les risques liés aux TIC, les cyber-risques, les risques liés aux données critiques et les risques découlant de la conception et de la mise en œuvre de la gestion de la continuité des activités (BCM), doivent être mises en œuvre en tenant compte de leurs tâches, compétences et responsabilités. 140

f. Contrôle

14 1 Afin d'évaluer les **mesures de contrôle et d'atténuation** existantes, il convient notamment de procéder à une évaluation régulière de l'efficacité des contrôles clés par un organisme d'audit indépendant et d'en consigner les résultats (ce que l'on appelle les *tests d'efficacité de la conception* et les *tests d'efficacité opérationnelle*). Les contrôles clés sont les mesures de contrôle et les mesures d'atténuation qui minimisent les risques inhérents jugés significatifs.

14 2 En outre, la **séparation fonctionnelle** des tâches, des compétences et des responsabilités doit être régulièrement vérifiée afin de garantir l'indépendance et d'éviter les conflits d'intérêts. Les évaluations des risques et des contrôles doivent prendre en compte les risques inhérents, l'efficacité des mesures de contrôle et d'atténuation existantes ainsi que les risques résiduels.

14 3 Avant toute **modification significative** des produits, activités, processus et systèmes, il convient de réaliser des évaluations ad hoc des risques et des contrôles, en tenant compte des risques opérationnels liés au processus de modification et à l'état cible. Si nécessaire, l'établissement doit adapter sa tolérance au risque et mettre en œuvre des mesures de contrôle et d'atténuation.

g. Rapports

14 4 Le **service de contrôle des risques** rend compte, au moins une fois par an à l'organe de haute direction et au moins une fois par semestre à la direction générale, des risques opérationnels au niveau le plus élevé de la catégorisation, de leur comparaison avec la tolérance au risque définie, ainsi que des détails relatifs aux pertes internes significatives.

14 5 En ce qui concerne les risques informatiques et cybernétiques pertinents, le **rapport** au moins annuel adressé à la direction contient en outre des informations sur l'évolution de ces risques, l'efficacité des contrôles clés correspondants ainsi que sur les événements internes et externes significatifs liés à ces risques.

h. Risques liés aux TIC

a. Stratégie et gouvernance

La gestion des **risques liés aux TIC** doit tenir compte des normes et pratiques internationalement reconnues en la matière, ainsi que de l'influence des nouvelles évolutions technologiques sur ces risques. 146

La **direction** veille à ce que des procédures, des processus et des contrôles, ainsi que des tâches, des compétences et des responsabilités, soient mis en œuvre et documentés tant pour la gestion du changement (appelée *« Change Management »*) que pour l'exploitation des TIC (appelée *« Run, Maintenance »*). Ceux-ci doivent être dotés de ressources qualifiées et adéquates. 147

b. Gestion des changements

Pour
toutes les phases de développement ou d'acquisition de systèmes TIC, la **gestion des changements** doit définir des procédures, des processus et des contrôles. À chacune de ces phases, elle doit tenir compte des répercussions du changement sur les risques liés aux TIC – en particulier les exigences en matière de confidentialité, d'intégrité et de disponibilité. 148

L'institut Fintech doit garantir une **séparation** entre l'environnement de développement ou de test et l'environnement de production des TIC. Cela inclut également une attribution claire des TIC et une réglementation des droits d'accès associés. 149

Lors du développement et de l'acquisition de TIC, les exigences fonctionnelles et non fonctionnelles doivent être clairement définies, d'être approuvées, puis testées et validées en fonction de leur **criticité**. 150

c. Exploitation des TIC

Dans le cadre de l'exploitation des TIC, l'établissement Fintech doit tenir un ou plusieurs inventaires des composants TIC. Cet **inventaire** comprend les composants matériels et logiciels ainsi que les emplacements de stockage des données critiques, et tient compte aussi bien des dépendances au sein de l'établissement que des interfaces avec les principaux prestataires externes. L'inventaire doit être disponible en temps réel et doit être régulièrement vérifié et mis à jour afin de garantir son exhaustivité et son exactitude. 151

15 2 En outre, l'établissement doit disposer de procédures, de processus et de contrôles garantissant la confidentialité, l'intégrité et la disponibilité de l'environnement de production TIC, en tenant compte de la **tolérance au risque** applicable.

15 3 Dans ce cadre, il convient de veiller à ce qu'en cas de perturbation ou d'interruption importante, l'établissement puisse assurer une transition sans heurts entre l'exploitation des TIC et ses processus de *plan de continuité des activités* (PCA) et de *plan de reprise après sinistre* (PRS). À cette fin, l'établissement met en œuvre des **procédures de sauvegarde et de restauration** appropriées, qui sont régulièrement testées et validées.

15 4 Enfin, l'établissement doit également mettre en œuvre des procédures, des processus et des contrôles garantissant une gestion des TIC fondée sur les risques lorsque la fin de vie opérationnelle est imminente ou que la date de mise hors service prévue a été dépassée.

d. Gestion des incidents

15 5 L'établissement fintech dispose de procédures, de processus et de contrôles pour traiter les **incidents informatiques majeurs**, y compris ceux résultant de dépendances vis-à-vis de prestataires externes essentiels et de l'externalisation au sein du groupe. À cet égard, l'ensemble du cycle de vie des incidents informatiques majeurs doit être pris en compte et il convient de définir les tâches, compétences et responsabilités nécessaires à la gestion de ces incidents.

15 6 La gestion des incidents informatiques significatifs doit être coordonnée et reliée aux **processus BCM et DRP**.

15 7 Les incidents informatiques que l'établissement classe comme perturbation majeure de l'exécution de ses processus critiques et qui revêtent une importance pour la surveillance doivent être signalés sans délai à la **FINMA**.

i. Risques cybernétiques

15 8 L'établissement doit également définir des tâches, des compétences et des responsabilités claires en matière de **risques cybernétiques**. À cet égard, il doit au moins couvrir les aspects suivants, conformément aux normes et pratiques internationalement reconnues, dont la mise en œuvre efficace doit

être assurée par des procédures, processus et contrôles, et dont le développement et l'amélioration continus doivent être assurés :

- identification du **potentiel de menace** spécifique à l'établissement lié aux cyberattaques et évaluation des conséquences possibles en cas d'exploitation des vulnérabilités concernant les composants inventoriés des TIC et les données électroniques critiques ;
- protection des composants des TIC et des données électroniques critiques répertoriés contre les cyberattaques par la mise en œuvre de **mesures de protection** appropriées (telles que les sauvegardes de données, les plans de reprise, la formation des collaborateurs à la cybersécurité, la participation à des programmes de « bug bounty » ou les audits de sécurité du code source), notamment en matière de confidentialité, d'intégrité et de disponibilité ;
- Enregistrement et détection en temps réel des cyberattaques sur la base d'un processus de **surveillance** systématique et continue des composants inventoriés des TIC et des données électroniques critiques ;
- **B réaction**B aux vulnérabilités identifiées et aux cyberattaques par l'élaboration et la mise en œuvre de processus appropriés permettant de prendre rapidement des mesures de confinement et de remédiation ; et
- garantie d'une **B reprise**B rapide du fonctionnement normal de l'activité après des cyberattaques grâce à des mesures adaptées.

La requérante doit présenter les contrôles du SCI pertinents relatifs aux risques de cybersécurité et fournir les pièces justificatives correspondantes (procédures, processus et contrôles permettant de détecter, de contenir et d'éliminer une telle cyberattaque) dans le cadre de l'**analyse des risques cybernétiques**. 159

Les cyber-risques font partie des risques opérationnels et ne doivent pas être assimilés aux risques liés aux TIC. Les cyber-risques sont soumis à des facteurs d'influence externes plus importants, tels que l'exploitation de vulnérabilités via différents vecteurs d'attaque, par exemple lors d'attaques par ransomware ou par déni de service distribué (DDoS), ainsi que les menaces internes. Les établissements doivent donc inclure dans leur gestion des risques une définition distincte des cyber-risques, qui rende compte de la nature du risque. 160

16 1 La gestion des cyber-risques doit garantir qu'une cyber-attaque réussie ou partiellement réussie soit analysée quant à son importance pour les composants TIC critiques, les données électroniques critiques et les processus critiques (y compris les services et fonctions externalisés), et que l'**obligation de déclaration** à la FINMA soit respectée. Il est important que l'entreprise de fintech soit immédiatement informée des cyberattaques réussies ou partiellement réussies concernant d'éventuels services TIC externalisés et puisse agir en conséquence, et pas seulement pour s'acquitter en temps utile de son obligation de déclaration envers la FINMA.

16 2 Une fois l'évaluation initiale de la criticité effectuée et une information préalable informelle transmise au Key Account Manager compétent de la **FINMA** dans un délai de 24 heures, la déclaration doit être transmise conformément au catalogue d'exigences de la plateforme d'enquête EHP (champs obligatoires) doit être transmise dans un délai de 72 heures. Une fois le traitement du cas achevé au sein de l'établissement, un rapport final sur les causes, correspondant au degré de gravité, doit être remis au service compétent de la FINMA. Dans ce cadre, la requérante doit exposer comment elle s'assure que l'obligation de signalement des cyberincidents réussis ou partiellement réussis de gravité moyenne, élevé ou grave.

16 3 La direction fait régulièrement réaliser **des analyses de vulnérabilité** (analyse visant à identifier les failles logicielles existantes et les failles de sécurité dans l'infrastructure informatique) **et des tests d'intrusion** (vérification ciblée et exploitation des failles logicielles et des brèches de sécurité dans les TIC). Ceux-ci doivent être réalisés par du personnel qualifié disposant de ressources adéquates. Il convient de prendre en compte tous les composants inventoriés des TIC qui sont accessibles via Internet. En outre, il faut tenir compte des composants inventoriés des TIC qui ne sont pas accessibles via Internet, mais qui sont nécessaires à l'exécution de processus critiques ou qui contiennent des données électroniques critiques. La fréquence de ces analyses et tests doit être définie dans la documentation correspondante.

16 4 Sur la base des menaces spécifiques à chaque établissement, il convient de mener des **exercices de cybersécurité** fondés sur les risques et les scénarios. Les résultats des exercices doivent être documentés et consignés sous une forme appropriée. L'étendue et le contenu de ces exercices sont régis par le principe de proportionnalité. Les établissements non

d'importance systémique devraient organiser au moins un exercice « table-top » annuel, c'est-à-dire une simulation d'un scénario sur papier (exercice sur papier).

j. Risques liés aux données critiques

L'établissement de fintech doit définir les grandes lignes de la gestion des risques liés aux **données critiques** qui le concernent et doit veiller au respect de ces dispositions. Les données critiques sont des données qui doivent faire l'objet d'une protection particulière et qui doivent donc être définies par l'établissement en fonction des risques. Les données critiques peuvent l'être tant en termes de confidentialité que d'intégrité ou de disponibilité et sont donc soumises à différents niveaux de criticité. 165

Les données critiques en termes de **confidentialité**, c'est-à-dire les données confidentielles, sont des informations commerciales ou des données relatives aux clients ou à des personnes physiques qui doivent être protégées contre tout accès non autorisé afin de préserver la vie privée ou la sécurité d'une personne ou d'une organisation. 166

Les données critiques en termes d'**intégrité ou de disponibilité** doivent être définies par l'établissement en fonction des risques. Le caractère critique de ces données se rapporte à la capacité de l'établissement à fonctionner de manière efficace et performante (ou tout simplement) de fonctionner. Ces données critiques sont donc indispensables au bon fonctionnement de l'établissement. Ces «données critiques pour la mission» comprennent, par exemple, les données figurant dans les rapports financiers (tant internes qu'externes), les rapports réglementaires, ainsi que les données nécessaires au processus décisionnel, à la mise en œuvre technique ou à la mesure de la performance de l'entreprise. Si ce type de données est endommagé, détruit ou devient inaccessible, l'établissement, ses entités et ses collaborateurs risquent de ne plus être en mesure de remplir leurs missions. 167

Les données critiques doivent être gérées tout au long de leur **cycle de vie**. Ce cycle de vie englobe les responsabilités en matière de données, la collecte, le lieu de stockage, la maintenance, la la conservation (rétention), la suppression et l'élimination. Il prend également en compte les aspects liés à la production, à l'enrichissement, au traitement et au transfert des données critiques. 168

169 Les incidents qui compromettent de manière significative la confidentialité, l'intégrité ou la disponibilité des données critiques doivent être signalés sans délai à la **FINMA**.

170 Lors de la sélection des **prestataires de services** qui traitent des données critiques (c'est-à-dire toute manipulation de celles-ci) ou qui peuvent y avoir accès, il convient d'accorder une grande importance à la diligence raisonnable (due diligence). Des critères clairs doivent être définis pour évaluer la manière dont les prestataires de services traitent les données critiques et vérifiés avant la conclusion du contrat. Les prestataires de services doivent faire l'objet d'une surveillance et d'un contrôle périodiques, axés sur les risques, dans le cadre du système de contrôle interne de l'établissement.

k. Gestion de la continuité des activités

171 Chaque domaine d'activité et d'organisation concerné doit, dans le cadre de l'*analyse d'impact sur l'activité* (BIA), identifier ses processus critiques et les ressources nécessaires à cet effet (notamment en matière de personnel, d'installations (p. ex. bâtiments, infrastructure des postes de travail), d'informations, de systèmes informatiques ou d'infrastructure informatique, etc.) et les soumettre à la FINMA.

172 Pour les processus critiques, l'établissement doit définir le *Recovery Time Objective* (RTO) et le *Recovery Point Objective* (RPO) en termes de délais et les soumettre à la FINMA. Ceux-ci doivent être coordonnés avec les prestataires nécessaires à cet effet. Le respect du RTO et du RPO doit être régi par des accords de niveau de service (SLA) ou des contrats, ou garanti par d'autres procédures, processus et contrôles appropriés.

173 L'établissement doit définir au moins un *PCA* et le soumettre à la FINMA ; ce plan doit également décrire les circonstances déclenchant sa mise en œuvre ainsi que les processus décisionnels, et tenir compte de la perte de ressources. L'acceptation des risques résiduels doit être documentée de manière appropriée.

174 L'établissement définit au moins un *DRP* dans le cadre du PCA. Si des processus critiques ou des parties de ceux-ci sont externalisés, le DRP doit tenir compte des dépendances externes, des dispositions contractuelles ainsi que des solutions alternatives. En cas de modifications importantes, le DRP doit être revu *ad hoc*, mais au moins une fois par an.

En cas de crise, une **cellule de crise** est chargée de prendre en charge la gestion de la crise jusqu'au rétablissement d'une situation normale. Les circonstances déclenchant la crise ainsi que les tâches, compétences et responsabilités de la cellule de crise doivent être définies au préalable, et l'organisation de crise doit être adaptée à l'activité commerciale et à la structure géographique de l'établissement. La joignabilité des responsables en cas de crise doit être garantie. L'établissement doit élaborer une **stratégie de communication** pour la communication interne et externe en situation de crise. 17 5

La mise en œuvre des plans de continuité des activités (BCP) et des plans de reprise après sinistre (DRP), ainsi que le bon fonctionnement de l'organisation de crise, doivent être vérifiés par des **tests réguliers**. À cette fin, il convient d'établir une planification systématique garantissant une couverture régulière. Différentes approches de test, d'intensité et d'efficacité variables, peuvent être choisies, comme par exemple des exercices sur table. 17 6

Les tests doivent porter sur différents **scénarios** graves mais plausibles et tenir compte des dépendances en matière de reprise des activités, y compris celles vis-à-vis de tiers internes ou externes. À cet égard, la capacité de détection technique doit être exposée dans le cadre du scénario concerné, par exemple en exploitant un système central de *Security Information and Event Management* (SIEM) qui offre une vue unifiée des événements de sécurité dans l'ensemble de l'environnement TIC et permet ainsi de détecter les menaces et d'y réagir plus efficacement. 17 7

Des **rapports** réguliers adressés à l'organe de direction suprême et à la direction fournissent des informations sur les activités de test et d'audit menées ainsi que sur leurs résultats. Ils mettent en évidence les priorités fixées (par exemple, la priorisation des processus critiques nécessaires à l'exécution des fonctions critiques) et les lacunes identifiées dans la couverture d'autres processus critiques. 17 8

l. Risques liés aux activités transfrontalières de prestation de services

Lorsque des établissements ou les sociétés de leur groupe fournissent **des services transfrontaliers** ou commercialisent des produits financiers au-delà des frontières, les risques découlant de l'application de législations étrangères (droit fiscal, droit pénal, droit en matière de blanchiment d'argent, 17 9

etc.) doivent être identifiés, limités et surveillés de manière appropriée. L'analyse des risques correspondante doit être soumise à la FINMA. Afin de garantir le respect des législations étrangères, des manuels pays correspondants doivent être présentés à la FINMA.

180 Les établissements soumettent leurs activités transfrontalières de prestation de services ainsi que la distribution transfrontalière de produits financiers à une analyse approfondie du cadre juridique et des risques qui y sont liés. Sur la base de cette analyse, les établissements prennent les **mesures** stratégiques et organisationnelles nécessaires pour éliminer et de minimiser les risques, et les adaptent en permanence à l'évolution du contexte. En particulier, ils disposent du savoir-faire spécifique à chaque pays nécessaire, définissent des modèles d'accompagnement adaptés à chaque pays, forment leurs collaborateurs et garantissent le respect des prescriptions par des mesures organisationnelles, directives, de modèles de rémunération et de sanctions. La directive transfrontalière correspondante doit être soumise à la FINMA.

181 Les risques liés aux gestionnaires de fortune externes, aux intermédiaires et aux autres prestataires de services doivent également être pris en compte. La **sélection et la formation** de ces partenaires doivent être effectuées avec le soin requis.

182 Ce principe s'applique également aux situations dans lesquelles une filiale, une succursale ou une entité similaire **domiciliée à l'étranger** d'un établissement suisse fournit des services transfrontaliers à la clientèle.

m. Résilience opérationnelle

183 L'établissement identifie ses fonctions critiques (opérations ou prestations stratégiquement les plus importantes) ainsi que leurs seuils de tolérance aux interruptions. Celles-ci sont approuvées par l'organe de direction. En outre, l'organe de direction approuve et surveille régulièrement les mesures visant à garantir la **résilience opérationnelle**. Il s'agit ici de la capacité à surmonter des chocs opérationnels significatifs en minimisant autant que possible leurs répercussions négatives et en y remédiant rapidement.

184 Dans le cadre de l'évaluation de la résilience opérationnelle, la requérante doit définir des **fonctions critiques** et indiquer une tolérance à l'interruption plus élevée (par exemple 1 à 5 jours) pour chaque fonction critique. Les

fonctions critiques doivent être délimitées par le BCM et une *tolérance à la perturbation* globale doit être définie.

Sur cette base, l'établissement doit définir des **mesures** appropriées visant à garantir la résilience opérationnelle, en tenant compte de scénarios graves mais plausibles. Il convient ici d'adopter une approche préventive comprenant des mesures préventives ciblées, la mise en place d'un modèle d'exploitation et un apprentissage continu d'apprentissage et d'amélioration continus, afin de rendre les fonctions critiques aussi résilientes que possible («Resilience by Design»). 185

4. Service spécialisé dans la lutte contre le blanchiment d'argent

Les établissements fintech sont soumis à la loi sur le blanchiment d'argent (LBA) (art. 2, al. 2, let. a, LBA). Les **obligations de diligence en matière de lutte contre le blanchiment d'argent** sont régies par le titre 5 de l'ordonnance de la FINMA sur le blanchiment d'argent (art. 3, al. 1, en liaison avec l'art. 43*a* OBA-FINMA). En outre, la circulaire FINMA 2016/7 « Identification par vidéo et en ligne » s'applique aux établissements fintech. 186

Les établissements fintech doivent notamment réaliser une **analyse des risques de blanchiment d'argent** comprenant différents éléments : l'analyse doit tout d'abord définir la tolérance au risque en excluant explicitement certains risques. Elle doit ensuite préciser comment les différents risques de blanchiment d'argent sont pris en compte. Enfin, l'établissement fintech doit définir des indicateurs et des seuils afin de pouvoir démontrer le respect de sa propre stratégie commerciale et de sa politique de gestion des risques, ainsi que leur évolution au fil des ans. L'analyse des risques contient ainsi les informations essentielles sur la gestion visée des risques de blanchiment d'argent. 187

Sur le fond, la conception de l'analyse des risques de blanchiment d'argent dépend fortement des activités commerciales effectives, tant sur le plan matériel que géographique, de l'établissement fintech. Les catégories de risques suivantes peuvent, dans certains cas, s'avérer pertinentes : a. structure de la clientèle (risques pays, segments de clientèle, proximité de la relation avec le client), b. nature de la relation client (structures complexes), c. activités commerciales (produits et services), d. relations d'affaires présentant des 188

risques accrus (PEP, sociétés de domicile), e. risques liés aux transactions et autres risques similaires.

18 9 Les intermédiaires financiers doivent disposer d'une **fonction appropriée** de lutte contre le blanchiment d'argent et le financement du terrorisme (y compris le contournement des sanctions). Les personnes chargées de ces tâches doivent avoir suivi une formation adéquate et disposer des ressources nécessaires pour pouvoir exercer leur fonction de manière adéquate. Les règles internes correspondantes doivent être consignées sous une forme appropriée et mises à la disposition des collaborateurs chargés de ces tâches. Les dispositions légales applicables doivent être mises en œuvre en interne.

19 0 Les établissements fintech ont la possibilité de bénéficier d'**allègements organisationnels** dans le domaine du service spécialisé en matière de blanchiment d'argent, pour autant que l'établissement remplisse également les conditions requises pour bénéficier d'allègements dans le domaine de la conformité et de la gestion des risques (art. 14*e*, al. 5, OB) et que l'objectif de la lutte contre le blanchiment d'argent et le financement du terrorisme ne s'oppose pas à ces allègements (cf. art. 75*a* OBA-FINMA). En fonction du risque de blanchiment d'argent, la FINMA peut autoriser d'autres allègements ou ordonner un renforcement des exigences (cf. art. 3, al. 2, OBA-FINMA).

5. Documentation et processus

19 1 En règle générale, les requérants doivent soumettre des directives (règlements du conseil d'administration ou directives de la direction) à présenter à titre de **documentation** :

- organisation générale et compétences en matière de gestion des risques (souvent décrites dans le règlement d'organisation) ;
- stratégie d'entreprise et politique de gestion des risques ;
- analyse des risques ;
- gestion générale des risques ;
- matrice de contrôle générale (y compris les compétences, les périodicités et le contenu des contrôles) ;
- risques opérationnels (y compris les risques liés aux TIC/cyberrisques, les risques liés aux données critiques, à la protection et à la sécurité des données, ainsi que la gestion de la continuité des activités [BCM]) ;

- conformité en général ;
- blanchiment d'argent et sanctions en particulier ;
- en cas d'activités à l'étranger : opérations transfrontalières, y compris les manuels par pays ;
- externalisation (et contrats d'externalisation correspondants) ;
- conservation des dépôts du public et surveillance du seuil de 100 millions de CHF ;
- comportement des collaborateurs ;
- traitement des avoirs en déshérence (cf. art. 37*l* et art. 37*m* LB ainsi que les art. 45 et suivants OB) ;
- en cas d'applicabilité de la FIDLEG : conduite vis-à-vis des clients.

6. Prévention des conflits d'intérêts

Les établissements Fintech doivent prendre les mesures organisationnelles appropriées pour éviter les **conflits d'intérêts** susceptibles de survenir lors de la fourniture de leurs services ou pour exclure tout préjudice pour les clientes et clients résultant de tels conflits. Si un conflit d'intérêts ne peut être exclu, il doit être divulgué (art. 14*g* OB) et les clients doivent en être informés en conséquence. Les intérêts propres des titulaires d'autorisation et de leurs collaborateurs ne doivent pas aller à l'encontre des intérêts des clients. De même, les intérêts des clients ne doivent pas entrer en conflit entre eux. 19 2

D. Exigences financières (al. 3, let. c)

1. Plan d'affaires

La requérante doit présenter un **plan d'affaires** comprenant un budget (bilan, compte de résultat) pour les trois prochains exercices, avec des scénarios optimiste, réaliste et pessimiste. La planification des liquidités pour le premier exercice doit être établie selon le scénario pessimiste du plan d'affaires (sur une base mensuelle). 19 3

Les établissements fintech doivent disposer d'un **modèle économique** garantissant le respect indépendant et durable de leurs obligations financières. Il convient d'éviter de fixer des critères d'autorisation trop bas et de faire preuve d'une propension au risque trop élevée. Si, pour des raisons 19 4

structurelles, un établissement ne peut dégager de bénéfices et ne peut exister qu'à l'aide de subventions des parties prenantes (à fonds perdu), il existe une situation irrégulière qui remet en cause l'éligibilité à l'autorisation. Dans ce cas, la pérennité de l'établissement dépend uniquement de la solvabilité et de la volonté des propriétaires économiques, ce qui constitue un risque inacceptable tant du point de vue de la protection des créanciers que de celle du bon fonctionnement de l'établissement. Même un excédent de fonds propres et la détermination des propriétaires économiques à couvrir, année après année, les pertes d'exploitation encourues, de sorte qu'il n'y ait pas de danger immédiat pour les créanciers, ne permettent pas, au regard de ces critères, , une rentabilité insuffisante persistante. Afin de prouver qu'elle est en mesure de respecter ces exigences, la requérante doit notamment présenter les scénarios économiques réalistes et fondés mentionnés ci-dessus.

19 5 La **surveillance** exercée par la FINMA ne garantit pas, en ce sens, le succès commercial des établissements surveillés, mais vise à protéger les clientes et clients. Dans le cadre de la procédure d'autorisation, la FINMA vérifie que les plans d'affaires et les plans de financement soient plausibles. Un tel examen est d'autant plus important que les clients de personnes visées à l'art. 1*b* LB ne sont pas protégés en cas de faillite de celles-ci (notamment parce que leurs créances sont subordonnées aux créances salariales) et que les faillites ne sont pas rares dans ce domaine et peuvent même survenir dès la phase de démarrage.

19 6 Lors de l'**analyse** correspondante du modèle économique, il convient notamment de prendre en compte les points suivants :

- identification des risques majeurs liés au modèle économique ;
- vérification de la capacité de l'établissement à s'adapter à d'éventuels changements de circonstances ;
- analyse des moyens financiers disponibles et des autres ressources nécessaires à la mise en œuvre de la stratégie ;
- évaluation de la stratégie et de l'appétit pour le risque de l'établissement ;
- prise en compte du contexte de marché et de l'environnement commercial, et comparaison des ambitions de croissance de la société avec celles d'autres prestataires ;

- vérification de la faisabilité ou de la plausibilité des hypothèses du plan d'affaires ;
- vérification de la rentabilité d'un établissement afin de garantir un rendement suffisant du capital et d'assurer la pérennité de ses activités (y compris une couverture adéquate des coûts de financement (fonds propres et capitaux empruntés) ainsi que des frais d'exploitation).

Si l'établissement fintech à évaluer fait partie d'un **groupe**, les critères susmentionnés doivent être examinés non seulement au niveau de l'établissement individuel, mais aussi au niveau du groupe. 197

2. Liquidité

Les établissements fintech doivent disposer de **moyens financiers** adéquats (art. 1*b*, al. 3, let. c, LB). Le champ d'activité et son étendue géographique doivent correspondre aux capacités financières de l'établissement fintech (art. 14*b*, al. 2, OB). 198

Pour des raisons de gestion des risques, la FINMA exige qu'un établissement fintech dispose, au moment de l'octroi de l'autorisation, de liquidités suffisantes pour couvrir au moins ses coûts fixes pendant la phase de démarrage, en tenant compte des éventuels revenus. À cette fin, l'établissement fintech doit présenter une **planification de la liquidité** (sur une base mensuelle) et, comme condition d'autorisation, des justificatifs (relevés bancaires, etc.) attestant de l'état actuel de ses liquidités. 199

Afin de garantir sa solvabilité, l'établissement fintech doit intégrer les **risques de liquidité** dans son système de gestion des risques et les surveiller en permanence dans le cadre du SCI. 200

3. Capital minimum

Pour obtenir une autorisation, un établissement fintech doit justifier du capital minimum fixé par le Conseil fédéral, intégralement libéré (art. 1*b*, al. 1, en liaison avec l'art. 3, al. 2, let. b, LB). Les établissements fintech doivent disposer d'un **capital minimum** correspondant à 3 % des dépôts du public reçus et des actifs cryptographiques détenus en dépôt collectif, avec un minimum de 300 000 CHF. Ce capital doit être entièrement libéré et maintenu en permanence. 201

20 2 Le capital minimum doit être utilisé aux **fins** de l'entreprise. Il ne peut donc pas être prêté à des participants qualifiés ou à des personnes physiques ou morales qui leur sont proches, ni être investi dans des participations contrôlées par ceux-ci (art. 17*a*, al. 1, OB). Cette restriction des possibilités d'investissement vise à réduire le risque de détournement (risque de fraude) au détriment de l'entreprise. Les dispositions de l'ORD et de l'ORL ne sont pas applicables en l'absence de transformation des échéances (art. 17*a*, al. 3, OB).

20 3 Il subsiste néanmoins certains **risques de liquidité et de contrepartie**. C'est pourquoi il faut également s'assurer que les personnes visées à l'art. 1*b* de la LB disposent de moyens financiers suffisants pour supporter leurs risques. Le capital minimum ne doit pas seulement garantir une certaine protection des dépôts, mais surtout assurer une infrastructure organisationnelle et technique adéquate de l'établissement.

20 4 La FINMA peut, dans des cas particuliers, fixer **des exigences de fonds propres plus élevées** si cela semble nécessaire au vu des risques liés à l'activité (art. 17*a*, al. 2, OB) . Le calibrage des exigences en matière de fonds propres vise à garantir une application équitable et uniforme de la loi pour l'ensemble des différents modèles d'activité. Le capital supplémentaire prévu à l'art. 17*a*, al. 2, OB doit permettre aux établissements agréés d'assurer une durée de survie minimale.

20 5 Afin de **prouver** qu'elle satisfait aux exigences financières, la requérante doit fournir les informations suivantes :

- des justificatifs appropriés attestant le respect des exigences en matière de capital minimum et une description de la manière dont le respect de ces exigences minimales est garanti en cas d'augmentation des dépôts du public ;
- l'évolution prévisionnelle du capital minimum en fonction du plan d'affaires, y compris des informations sur les sources de financement.

E. Garantie (al. 3, let. d)

20 6 Les personnes chargées de fonctions au sein des organes – aux trois niveaux que sont l'actionnariat qualifié, la direction et le conseil d'administration – doivent jouir d'une bonne réputation et offrir **la garantie d'une activité**

irréprochable (art. 1*b*, al. 3, let. d, LB) (appelées «personnes de garantie») . L'examen de la garantie porte à la fois sur l'aptitude professionnelle (« fitness ») à exercer la fonction concrète et sur l'intégrité personnelle (« properness ») de ces personnes. Afin de vérifier la garantie et la bonne réputation, des informations et des documents sont exigés avec la demande concernant les personnes de garantie (cf. art. 8 OB).

Afin de prouver que les exigences applicables aux membres de l'organe chargé de la gestion et de la direction sont remplies, les **documents** suivants doivent être fournis : 20 7

- Données personnelles ;
- copie d'une pièce d'identité en cours de validité (copie signée et datée du passeport ou de la carte d'identité) ;
- copie du permis de séjour ou d'établissement pour les ressortissants étrangers (copie signée et datée) ;
- extrait du casier judiciaire (datant de moins de 3 mois) ;
- extrait du casier judiciaire du pays de résidence antérieur et/ou du pays d'origine pour les ressortissants étrangers résidant en Suisse depuis moins de 5 ans (datant de moins de 3 mois) ;
- extrait du registre des poursuites ou attestation équivalente (datant de moins de 3 mois) ;
- CV signé par la personne concernée (comprenant des informations sur la formation initiale et continue ainsi que sur au moins deux références) ; Relevé et description des activités professionnelles et mandats passés et actuels, y compris les années et les dates) ;
- Contrat avec la requérante (signé et daté) ;
- Déclaration concernant les procédures en cours et clôturées (formulaire B1, signé et daté) ;
- déclaration relative aux participations qualifiées (formulaire B3, signé et daté) ;
- déclaration relative aux autres mandats (formulaire B3, signé et daté).

208 À cet effet, la FINMA exige de la requérante qu'elle lui fournisse (en utilisant les **formulaires** prévus à cet effet par la FINMA) les informations suivantes **concernant les participations, c'est-à-dire l'actionnariat** :

- capital social (structure, répartition, valeur nominale, libération, etc.) ;
- liste de tous les participants détenant une participation directe ou indirecte de 5 % ou plus (jusqu'à l'ayant droit économique, avec indication des droits de vote et de la participation au capital) ;
- représentation graphique de tous les actionnaires qualifiés, directs ou indirects, jusqu'aux ayants droit économiques (avec indication du montant de chaque participation), ventilée selon les parts de droits de vote et de capital ;
- informations sur d'éventuels accords ainsi que sur d'autres possibilités de contrôle ou d'influence déterminante ; les documents tels que les conventions d'actionnaires ou les contrats d'investissement doivent être fournis ;
- déclaration relative aux détenteurs de participations qualifiées (formulaire A1 ; à fournir par le requérant) ;
- annexe à la déclaration relative aux détenteurs de participations qualifiées (formulaire A2 ; par participant qualifié ; à fournir par le requérant).

209 **Les détenteurs de participations qualifiées** doivent également jouir d'une bonne réputation et garantir que leur influence ne porte pas atteinte à une activité commerciale prudente et solide. Ils ne doivent toutefois pas nécessairement être indépendants de la direction. Est considéré comme détenteur d'une participation qualifiée quiconque détient au moins **10 %** des voix ou du capital ou peut exercer une influence déterminante sur l'activité commerciale d'une autre manière (art. 14*d*, al. 3 OB). La variante de l'influence «d'une autre manière» ne sert pas seulement à expliquer l'objectif de la norme, mais revêt également une importance propre. Elle vise à prendre en compte d'autres influences factuelles et juridiques, indépendamment des seuils fixés.

210 À partir d'une participation supérieure à **5 %**, les justificatifs énumérés dans les sont exigées.

Les justificatifs à fournir par les personnes physiques en tant que **participants qualifiés**, directs ou indirects, comprennent : 21 1

- les données personnelles ;
- une copie d'une pièce d'identité valide (copie du passeport ou de la carte d'identité signée et datée par le titulaire) ;
- extrait du casier judiciaire (datant de moins de 3 mois) ;
- extrait du casier judiciaire de l'État de résidence antérieur et/ou d'origine pour les ressortissants étrangers résidant en Suisse depuis moins de 5 ans (datant de moins de 3 mois) ;
- extrait du registre des poursuites ou attestation équivalente (datant de moins de 3 mois) ;
- CV signé par la personne concernée (comprenant des informations sur la formation initiale et continue ainsi que sur au moins deux références, la liste et la description des activités professionnelles passées et actuelles ainsi que des mandats, avec indication des années et des dates) ;
- Déclaration précisant si la participation qualifiée est détenue pour son propre compte ou à titre fiduciaire pour le compte de tiers, et si la personne concernée a accordé des options ou des droits similaires pour cette participation (formulaires « Déclaration des personnes directement / indirectement qualifiées », signés et datés) ;
- déclaration concernant les procédures en cours et clôturées (formulaire B1, signé et daté) ;
- déclaration relative aux participations qualifiées (formulaire B2, signé et daté).

Les pièces justificatives requises pour les **personnes morales** en tant que détenteurs qualifiés directs ou indirects comprennent : 21 2

- une description détaillée de l'organisation, des activités commerciales, de la situation financière (y compris les derniers comptes annuels, s'ils sont disponibles) et, le cas échéant, de la structure du groupe ;
- extrait du registre des poursuites ou attestation équivalente (datant de moins de 3 mois) ;
- extrait du registre du commerce ou attestation correspondante ;

- déclaration indiquant si la participation qualifiée est détenue pour compte propre ou à titre fiduciaire pour le compte de tiers et si la personne détenant une participation qualifiée a accordé des options ou des droits similaires pour cette participation (formulaires A3/A4, signés et datés) ;
- Déclaration concernant les procédures en cours et clôturées (formulaire B1, signé et daté) ;
- Déclaration relative aux participations qualifiées (formulaire B2, signé et daté).

F. Présentation des comptes et révision comptable (al. 4, let. a, b et c)

21 3 La **présentation des comptes** et la révision des comptes annuels sont régies exclusivement par les dispositions du CO (art. 1*b*, al. 4, let. a, LB), la révision restreinte étant obligatoire (pas de possibilité de dérogation au sens de l'art. 727*a*, al. 2 à 5, CO) (art. 1*b*, al. 4, let. b, LB) . Si les dépôts du public ne sont pas séparés des fonds propres, un contrôle ordinaire doit être effectué (art. 14*f*, al. 1, let. b, OB). Dans l'idéal, l'établissement procède à un contrôle ordinaire conformément à l'art. 727 CO.

21 4 Les établissements fintech doivent mandater une **société d'audit** agréée pour effectuer le contrôle prudentiel prévu à l'art. 24 LFINMA (art. 1*b*, al. 4, let. c, LB). À cette fin, ils doivent désigner une société d'audit agréée au sens de l'art. 9a LSR (cf. art. 24, al. 1, let. a, LFINMA). La demande d'autorisation doit être accompagnée d'une déclaration d'acceptation de la société d'audit prudentielle ainsi que d'un questionnaire rempli concernant les prestations des sociétés d'audit agréées, disponible sur le site Internet de la FINMA.

G. Obligations d'information (al. 4, let. d)

21 5 Les dispositions relatives aux dépôts privilégiés et au remboursement immédiat (art. 37*a* et art. 37*b* LB) (garantie des dépôts) ne s'**appliquent pas** aux dépôts du public et aux actifs cryptographiques acceptés par un établissement fintech. Avant l'acceptation des dépôts, les déposants doivent être informés de l'**absence de garantie des dépôts et** de l'**absence de protection en cas de faillite**, et être informés des conséquences possibles (art. 1*b*, al. 4, let. d, LB) .

Conformément à l'art. 7*a*, al. 1, OB, les clients doivent être informés par écrit ou sous une autre **forme vérifiable** (sur un document séparé, dans la documentation relative au modèle d'affaires ou encore séparément par e-mail) de l'absence de garantie des dépôts ainsi que du modèle d'affaires des établissements fintech, de leurs prestations et des risques liés aux technologies utilisées. 216

Les clients doivent être informés de manière à disposer, **avant la conclusion du contrat**, d'un délai suffisant pour comprendre les informations en vue de la conclusion du contrat (art. 7*a*, al. 2, OB). Une simple information par le biais des conditions générales ne suffit pas (art. 7*a*, al. 3, OB). 217

Si les informations sont mises à disposition **par voie électronique**, les personnes visées à l'art. 1*b* de la LB doivent veiller à ce qu'elles puissent être consultées, téléchargées et enregistrées à tout moment sur un support durable dans toutes les langues (officielles) pertinentes des clients cibles (art. 7*a*, al. 4, OB). Sont considérés comme supports de données durables le papier et tout autre support permettant le stockage et la reproduction à l'identique d'une information (art. 7*a*, al. 5, OB). 218

La requérante doit fournir à la FINMA des informations sur les renseignements communiqués aux clients conformément à l'art. 7*a* OB. À cette fin, il convient en règle générale de fournir le texte correspondant ainsi que le **processus d'onboarding** associé, y compris des captures d'écran des différentes étapes. Les informations relatives aux risques liés au modèle d'affaires, aux prestations et aux technologies utilisées doivent être détaillées. La mention indiquant que les dispositions relatives aux dépôts privilégiés (art. 37*a* LB), au remboursement immédiat (art. 37*b* LB) et à la garantie des dépôts (art. 37*h* s. LB) doit être complète et mise en évidence. Sur le plan procédural, l'information doit être conçue de telle sorte que, si l'accord n'est pas donné, la procédure d'onboarding du client soit interrompue. Une simple référence à l'art. 7*a* OB ne suffit en aucun cas. Les clients doivent accepter activement l'information (par exemple en cochant une case d'un simple clic de souris). 219

V. CAS PARTICULIERS (Y COMPRIS LES AL. 5 ET 6)

A. Augmentation éventuelle du seuil applicable aux dépôts du public par la FINMA (al. 5 et 6)

220 Si les dépôts du public dépassent le seuil de 100 millions de francs suisses, cela doit être signalé à la FINMA dans un délai de 10 jours et une **demande d'autorisation bancaire** au sens de l'art. 1*a* LB doit être déposée dans un délai de 90 jours (sous réserve de l'al. 5) (art. 1*b*, al. 6, LB) . Cette disposition transitoire ne semble pas nécessaire, puisqu'une personne visée à l'art. 1*b* LB est déjà soumise à la surveillance de la FINMA et entretient avec elle des échanges réguliers, de sorte qu'un rapprochement du seuil de 100 millions de CHF peut sans autre être signalé en temps utile dans ce contexte.

221 Le Conseil fédéral peut adapter le montant de **100 millions de CHF** en tenant compte de la compétitivité et de la capacité d'innovation de la place financière suisse (art. 1*b*, al. 2, LB). Dans des cas particuliers justifiés, la FINMA a également la possibilité de de déroger au plafond de 100 millions de CHF : ainsi, dans des cas particuliers, elle peut déclarer les alinéas 1 à 4 applicables également aux personnes qui acceptent à titre professionnel des dépôts du public supérieurs à 100 millions de CHF ou qui s'engagent publiquement à ne ni les placer ni les rémunérer, et à garantir la protection des clients par des mesures particulières (art. 1*b*, al. 5, LB).

B. Combinaison avec d'autres catégories d'autorisation

222 La combinaison d'une activité d'établissement fintech avec une activité de **maison de courtage** n'est en principe pas exclue. Il en va de même pour l'activité de **gestionnaire de fortune**, bien qu'il existe diverses questions de coordination réglementaire :

- il convient notamment de noter que l'autorisation fintech se situe en dehors de la **cascade d'autorisations** (cf. art. 6 LEFin) ;
- en cas de combinaison de catégories d'autorisation, ce sont les **exigences en matière de fonds propres** les plus élevées des deux catégories d'autorisation qui s'appliquent ;
- en cas de combinaison d'une autorisation « fintech » avec une autorisation de société de valeurs mobilières, la difficulté opérationnelle réside enfin

dans le traitement différent des dépôts : alors qu'il n'existe pas de garantie des dépôts pour les établissements « fintech » (art. 1*b*, al. 4, let. d, LB), les clients des sociétés de valeurs mobilières tenant des comptes de règlement bénéficient de la **garantie des dépôts**, ce qui nécessite une séparation des comptes de trésorerie respectifs. Pour les personnes visées à l'art. 1*b* LB, la solution la plus appropriée consisterait donc à exercer une éventuelle activité de courtage pour le compte de clients par l'intermédiaire d'une personne morale distincte.

C. Surveillance consolidée

Les dispositions de la Loi sur les banques (LB) relatives à la surveillance consolidée s'appliquent par analogie aux personnes visées à l'art. 1*b* LB, sous réserve des règles particulières prévues à l'art. 1*b*, al. 1, LB. Cela vaut également pour le droit de la consolidation bancaire prévu aux art. 3*b* et suivants de la LB et aux art. 21 et suivants de l' OB. Si une personne au sens de l'art. 1*b* LB fait partie d'un groupe financier, l'octroi de l'autorisation peut être subordonné à une **surveillance consolidée** appropriée par une autorité de surveillance des marchés financiers (art. 1*b*, al. 1, en liaison avec l'art. 3*b* LB). 22 3

La **circulaire FINMA 2025/4** « Surveillance consolidée des groupes financiers selon la LB et LEFin » expose la pratique de l'autorité de surveillance en matière d'assujettissement à la surveillance consolidée, ainsi que son étendue et son contenu. Par application par analogie, cette circulaire s'adresse également aux groupes financiers dominés par des personnes au sens de l'art. 1*b* LB et aux personnes au sens de l'art. 1*b* LB qui font partie d'un groupe financier (art. 1*b*, al. 1, en relation avec l'art. 3*c*, al. 1, LB) . 22 4

La FINMA peut donc exiger une surveillance consolidée du groupe dans le cas de **situations relevant d'un groupe**. Si d'autres autorités étrangères revendiquent simultanément la surveillance totale ou partielle du groupe financier, la FINMA s'accorde avec celles-ci, dans le respect de ses compétences, sur les compétences, les modalités et l'objet de la surveillance du groupe. Avant de prendre sa décision, elle entend les entreprises du groupe financier constituées en Suisse (art. 3*d*, al. 2, LB). 22 5

Sont considérées comme un **groupe financier** au sens de la présente disposition deux ou plusieurs entreprises lorsque : a) au moins une entreprise exerce une activité en tant que personne au sens de l'art. 1*b* LB ou est titulaire 22 6

d'une autorisation fintech ; b) elles exercent principalement leurs activités dans le secteur financier ; et c) elles forment une entité économique *ou* si, en raison d'autres circonstances, il y a lieu de supposer qu'une ou plusieurs des entreprises soumises à une surveillance individuelle sont légalement tenues ou de fait contraintes de venir en aide à des sociétés du groupe (art. 1*b*, al. 1, en relation avec l'art. 3*c*, al. 1, de la LB).

22 7 Une **obligation de soutien** juridique ou de fait au sens de l'art. 21, al. 2, OB peut notamment résulter des circonstances suivantes :

- des liens stratégiques, personnels, organisationnels ou financiers ;
- des coopérations et des dépendances ;
- l'utilisation d'une raison sociale commune ;
- une présence uniforme sur le marché ; ou
- des lettres de patronage, des accords « keep-well » ou des garanties similaires.

22 8 Les situations énumérées ne constituent pas une liste exhaustive. Ainsi, d'autres liens peuvent également donner lieu à une obligation de soutien de fait si ceux-ci sont susceptibles de donner à des tiers l'impression d'un **système d'affiliation**. Plus le taux de participation est élevé, moins les autres éléments de lien doivent être importants pour justifier, dans l'appréciation globale, l'intégration dans la surveillance consolidée.

22 9 Est considéré comme exerçant une activité dans le **secteur financier** au sens de l'art. 4, al. 1, OB quiconque : a) fournit ou négocie des prestations de services pour des opérations financières, notamment exerce, pour son propre compte ou pour le compte de tiers, des activités de dépôt ou de crédit, de négoce de valeurs mobilières, de placement de capitaux ou de gestion de fortune, ou accepte des actifs cryptographiques au sens de l'art. 5*a* OB ; b) détient des participations qualifiées principalement dans des entreprises actives dans le secteur financier (société holding) ; ou c) est une société du groupe importante au sens de l'art. 3*a* OB.

23 0 Les **activités** énumérées nommément à l'art. 4, al. 1, let. a, OB ne constituent pas une liste exhaustive. D'autres activités commerciales peuvent donc également relever du secteur financier. Il s'agit notamment du crédit-bail, de l'affacturage, des opérations par carte de crédit, de la participation à des

émissions, ainsi que de la conservation de titres, des services de paiement et de l'émission et de la conservation de moyens de paiement (y compris les jetons de paiement). Aux fins de la surveillance consolidée, les sociétés du groupe qui exercent des activités purement commerciales, industrielles ou administratives sont considérées comme n'opérant pas dans le secteur financier.

Des entreprises forment une **entité économique** lorsque l'une d'entre elles détient, directement ou indirectement, plus de la moitié des voix ou du capital des autres entreprises, ou les contrôle d'une autre manière (art. 21, al. 1, OB). Conformément à l'art. 21, al. 2, OB, une obligation de soutien peut notamment résulter : a) de liens personnels ou financiers ; b) de l'utilisation d'une raison sociale commune ; c) d'une présence commune sur le marché ; ou d) de lettres de patronage. Les sociétés du groupe sont des entreprises liées par une entité économique ou par une obligation de soutien (art. 22 OB). 23 1

L'intégration d'une société dans la surveillance consolidée peut également être déclenchée en l'absence de participation majoritaire (« contrôlée d'une autre manière »), pour autant que d'autres éléments de nature juridique ou factuelle indiquent l'existence d'un système d'interdépendance. Sont notamment considérés comme tels les liens en matière de personnel, d'organisation, financières ou commerciales **interdépendances et liens**. Si une personne au sens de l'art. 1*b* LB est contrôlée par une ou plusieurs personnes physiques qui contrôlent d'autres sociétés soumises à la surveillance de la FINMA ou d'autres sociétés importantes actives dans le secteur financier, il peut s'agir, dans certaines circonstances, d'un groupe financier dit *de facto*, qui doit être soumis à une surveillance consolidée. 23 2

La FINMA peut soumettre un groupe financier à la **surveillance des groupes** si celui-ci : a) gère en Suisse une personne organisée selon le droit suisse au sens de l'art. 1*b* LB ; ou b) est effectivement dirigé depuis la Suisse (art. 1*b*, al. 1, en relation avec l'art. 3*d*, al. 1, LB). La surveillance des groupes exercée par la FINMA s'étend à l'ensemble des sociétés du groupe actives dans le secteur financier (art. 23, al. 1, OB). 23 3

Dans des cas justifiés, la FINMA peut **exclure** des sociétés du groupe du secteur financier de la surveillance consolidée ou déclarer que ses dispositions ne leur sont que partiellement applicables, notamment lorsqu'une société du groupe n'est pas significative pour la surveillance consolidée (art. 23 4

23, al. 2, OB) . La FINMA peut **inclure**, en tout ou en partie, dans la surveillance consolidée une entreprise du secteur financier qui est contrôlée conjointement par un groupe financier soumis à la surveillance de la FINMA et par des tiers (art. 23, al. 3 OB).

23 5 Pour des raisons liées à la protection des investisseurs et des créanciers, la FINMA part, dans le cas de structures de groupes comprenant des établissements fintech, du **principe de la surveillance consolidée**, tout en tenant compte des risques spécifiques à chaque cas particulier.

23 6 La définition du **périmètre de consolidation** pour la surveillance consolidée de la FINMA s'effectue en concertation avec l'autorité de surveillance étrangère compétente, conformément à l'art. 3*d*, al. 2, LB, et comprend notamment la détermination de l'autorité de surveillance principalement compétente (*Lead Regulator*). En outre, il est inhérent à la surveillance consolidée que toutes les autorités de surveillance concernées se concertent sur les compétences et les modalités de la coopération. Les modalités de la coopération en matière de surveillance et de l'échange d'informations sont fixées au cas par cas ou de manière générale entre les autorités de surveillance. Cela permet d'éviter toute lacune ou tout double emploi.

23 7 Afin de traiter les risques à l'échelle du groupe, la FINMA peut, en appliquant le principe de proportionnalité, au lieu de recourir à la surveillance consolidée ou de refuser l'octroi d'une autorisation, imposer des mesures structurelles préventives appropriées visant à **isoler** (*ring fencing*) les risques ou d'autres mesures (par ex. l'adaptation de la structure du groupe).

23 8 En cas de contrôle étranger, l'accord des **autorités de surveillance étrangères** compétentes doit toutefois être obtenu dans tous les cas (cf. art. 1*b*, al. 1, en liaison avec l'art. 3bis, al. 1bis, LB). La surveillance consolidée doit en principe porter sur tous les aspects de la surveillance (consolidation qualitative et quantitative).

23 9 En cas d'activité de groupe, le requérant doit :

- fournir un **organigramme** du groupe comprenant des informations sur les autorisations existantes ou prévues en vertu de la législation sur les marchés financiers, une représentation graphique ainsi que les parts de droits de vote et de capital ; ainsi qu'

- une description détaillée de tous les **liens** stratégiques, en matière de personnel, d'organisation ou financiers entre la requérante et toutes les sociétés du groupe.

D. Situations transfrontalières

Les établissements fintech peuvent exercer leurs activités à l'étranger, être sous contrôle étranger et/ou appartenir à un groupe financier étranger. Se pose en outre la question de la réciprocité et de la reconnaissance de catégories d'autorisations étrangères comme équivalentes à l'autorisation fintech, et donc celle de savoir si des succursales et des représentations sont possibles. 240

1. Activité à l'étranger (*outbound*)

Les établissements fintech peuvent exercer une **activité à l'étranger** active ou simplement passive, au sens d'une prestation de services transfrontalière. Toute activité à l'étranger entraîne, pour les établissements fintech, une augmentation des risques liés à l'activité commerciale et un élargissement du périmètre de conformité. En conséquence, les risques découlant de l'application de la législation étrangère (législation fiscale, pénale, sur le blanchiment d'argent, etc.) doivent être identifiés, classés et limités de manière appropriée au moyen d'une analyse des risques (mesures stratégiques et organisationnelles, savoir-faire, modèles de services par pays, formations, sélection des partenaires) et contrôlés (au moyen de directives, de modèles de rémunération et de sanctions) . 241

En raison de la législation étrangère, une **activité internationale active** présuppose généralement la mise en place d'une forme d'organisation administrative locale de l'établissement fintech à l'étranger. Par conséquent, les établissements fintech organisés selon le droit suisse doivent adresser une notification à la FINMA avant de créer à l'étranger une filiale, une succursale, une agence ou une représentation (art. 1*b*, al. 1, en relation avec l'art. 3, al. 7, LB). La déclaration qu'un établissement de fintech doit adresser à la FINMA avant de commencer son activité à l'étranger doit contenir toutes les informations et tous les documents nécessaires à l'évaluation de cette activité, à savoir : a) un plan d'affaires décrivant notamment la nature des activités prévues et la structure organisationnelle, b) l'adresse de l'établissement étranger, c) les noms des personnes chargées de l'administration et de la 242

direction, d) la société d'audit, e) l'autorité de surveillance du pays d'accueil (art. 20, al. 1, OB) . L'établissement de fintech doit en outre signaler la cessation ou toute modification substantielle de l'activité à l'étranger, ainsi que le changement de société d'audit ou d'autorité de surveillance (art. 20, al. 2, OB).

24 3 Même dans le cas d'une **activité à l'étranger** purement passive, celle-ci doit être présentée dans le registre des établissements (OGR) sous la forme d'une description précise, tant sur le plan matériel que géographique, du champ d'activité (cf. art. 1*b*, al. 3, let. a de la LB ; art. 14*b*, al. 1 de l'Ordonnance sur les banques). Il en résulte des exigences accrues en matière d'organisation administrative interne et de gouvernance d'entreprise. À cet égard, il est exigé que les risques et contrôles correspondants soient pris en compte dans l'organisation et la documentation de la gestion des risques ainsi que de la conformité. Cela inclut généralement, en particulier, une directive transfrontalière comprenant des « Country Manuals » (guides par pays) pour les pays concernés. Si des établissements fintech déjà agréés souhaitent désormais exercer une activité passive à l'étranger, cela constitue une modification substantielle des éléments justifiant l'autorisation et doit donc faire l'objet d'une autorisation préalable (cf. art. 8*a*, al. 2, OB). Il n'est pas possible de commencer l'activité dans l'OGR à titre provisoire.

2. Contrôle étranger

24 4 La FINMA peut subordonner l'autorisation de créer un établissement de fintech, qui doit être organisé selon le droit suisse, mais sur lequel pèse toutefois une **influence étrangère dominante** (cf. à ce sujet l'art. 3bis, al. 3, LB) – par exemple par le biais d'actionnaires ou de sociétés du groupe ayant leur siège à l'étranger – aux conditions supplémentaires suivantes (art. 1*b*, al. 1 en relation avec l'art. 3bis, al. 1, LB) :

1. de la garantie de la **réciprocité** par les États dans lesquels les étrangers détenant des participations qualifiées ont leur domicile ou leur siège (cf. art. 19, al. 1, OB), pour autant qu'aucune obligation internationale contraire ne s'y oppose (cf. art. 3^{quater} LB) ; ainsi que

2. de l'utilisation d'une **raison sociale** qui ne fait pas référence au caractère suisse de l'établissement de fintech ou qui ne permet pas de le déduire.

Il en va de même pour les établissements de fintech qui, après leur création, sont contrôlés par des étrangers ou lorsque les étrangers détenant des participations qualifiées changent (art. 1*b*, al. 1, en liaison avec l'art. 3[ter], al. 1 et 2, de la LB) . Les demandes d'**autorisations complémentaires** en tant qu'établissement fintech sous contrôle étranger doivent contenir les informations prévues à l'art. 8 OB (art. 18 OB). 245

3. Représentations (*inbound*)

En application du renvoi général par analogie prévu à l'art. 1*b*, al. 1, LB, les dispositions de la LB s'appliquent par analogie aux succursales établies en Suisse ou aux représentants désignés par des «personnes étrangères au sens de l'art. 1*b* LB» (art. 1*b*, al. 1, en liaison avec l'art. 2, al. 1 LB). Conformément à l'art. 2, al. 1, LB, l'ordonnance sur les banques étrangères-FINMA (OBE-FINMA) s'applique par analogie également aux établissements fintech. 246

Sont donc considérées comme des «**personnes étrangères** au sens de l'art. 1*b* LB» toutes les entreprises de droit étranger qui détiennent à l'étranger une autorisation reconnue comme équivalente à l'autorisation fintech ou qui exercent l'activité d'une «personne au sens de l'art. 1*b* LB» (art. 1*b*, al. 1, en liaison avec l'art. 2 LB et l'art. 1, al. 1, OEB-FINMA). 247

Une «personne étrangère au sens de l'art. 1*b* LB» doit obtenir une **autorisation** de la FINMA si elle emploie en Suisse des personnes qui, pour son compte, concluent de manière durable et à titre professionnel des affaires en Suisse ou à partir de la Suisse, gèrent des comptes clients ou engagent juridiquement celle-ci (ce qu'on appelle une succursale) ou si elle agit d'une autre manière pour le compte des «personne étrangère au sens de l'art. 1*b* de la LB», notamment en lui transmettant des ordres de clients ou en la représentant à des fins publicitaires ou autres (ce qu'on appelle une «représentation») (art. 1*b*, al. 1, en liaison avec l'art. 2 de la LB et l'art. 2, al. 1, de l'OAB-FINMA). 248

L'OAB-FINMA n'est pas applicable lorsque la «personne étrangère au sens de l'art. 1*b* LB» est effectivement dirigée depuis la Suisse ou exerce ses activités exclusivement ou principalement en Suisse ou à partir de la Suisse, car les **obligations d'autorisation ordinaires** de la LB s'appliquent alors (cf. art. 1, al. 2, OAB-FINMA). 249

250 L'art. 19, al. 2, OB précise que, lors de la désignation d'une **représentation** permanente d'une «personne étrangère au sens de l'art. 1*b* LB», la réciprocité est également garantie lorsque les banques suisses peuvent ouvrir, dans l'État étranger, des représentations permanentes exerçant les mêmes fonctions. L'art. 19, al. 2, de l'Ordonnance sur les banques (OB) n'exige donc pas que les intermédiaires financiers suisses puissent également ouvrir des représentations à l'étranger. En outre, le Conseil fédéral est habilité, sur la base de la reconnaissance mutuelle de réglementations et de mesures prudentielles équivalentes, à conclure des traités internationaux prévoyant que « les personnes étrangères au sens de l'art. 1*b* LB » des États contractants puissent ouvrir une succursale ou une représentation sans autorisation de la FINMA (art. 1*b*, al. 1, en relation avec l'art. 2, al. 3, LB). Inversement, la FINMA peut soumettre intégralement les « personnes étrangères au sens de l'art. 1*b* LB » aux dispositions applicables aux établissements fintech suisses, pour autant que le droit du pays où ces « personnes étrangères au sens de l'art. 1*b* LB» n'accorde pas aux établissements fintech suisses des allègements équivalents et qu'aucun traité international ne s'y oppose (cf. art. 3, al. 2, OAB-FINMA).

251 Dans un premier temps, la question se pose de savoir quelles formes juridiques étrangères correspondent aux critères d'octroi de l'autorisation fintech. Si une **équivalence** à cet égard – et donc une obligation d'autorisation – est confirmée, la question se pose ensuite de savoir si tant une succursale qu'une représentation peuvent faire l'objet d'une autorisation en application par analogie de l'OAB-FINMA.

VI. MODIFICATIONS DE L'AUTORISATION

252 Les établissements fintech doivent signaler à la FINMA toute **modification** des faits sur lesquels repose l'autorisation (art. 8*a*, al. 1, OB) à la FINMA. Si les modifications sont importantes, une autorisation préalable de la FINMA doit être obtenue pour la poursuite de l'activité (art. 8*a*, al. 2, OB). Des modifications matérielles importantes du modèle d'affaires pendant la durée de la relation de surveillance (p. ex. modification du modèle d'affaires) peuvent, le cas échéant, nécessiter une adaptation du règlement d'exploitation et, le cas échéant, des statuts.

253 Dans les **directives de la FINMA** relatives à l'autorisation des fintechs, le ch. II énumère, sans que cette liste soit exhaustive, ce qui est considéré comme

une modification d'importance significative au sens de l'art. 8*a*, al. 2, OB et qui nécessite donc une autorisation préalable de la FINMA. Sont concernées les modifications suivantes :

- modification concernant les documents organisationnels (notamment les statuts et le règlement d'organisation ; cf. également l'art. 10, let. a, de l'ordonnance sur les établissements financiers (OEF);
- modifications concernant les participants qualifiés (cf. plus en détail l'art. 10, let. d et e, OEF);
- modifications concernant les personnes chargées de l'administration ou de la direction (cf. également l'art. 10, let. b, OEF);
- modifications concernant l'organisation (par exemple, modifications du contrôle des risques ou de la fonction de conformité) ;
- le cas échéant : modifications de l'infrastructure technique relative à la conservation d'actifs cryptographiques ;
- modification concernant les règles internes de gouvernance d'entreprise (Corporate Governance) ;
- modification concernant l'activité et les services accessoires (domaine d'activité) ;
- modification concernant l'externalisation de services essentiels ;
- démarrage, modification ou cessation d'activités à l'étranger (les filiales, succursales et représentations doivent toujours être mentionnées dans le registre du commerce) ;
- fusion, scission, transformation ou transfert de patrimoine conformément à la loi sur la fusion du 3 octobre 2003 (LFus) ; ainsi que
- changement de société d'audit en Suisse et à l'étranger.

La **demande** d'autorisation de modification doit contenir une justification détaillée (y compris une analyse des risques). Toutes les informations pertinentes doivent être documentées et les documents modifiés doivent également être joints dans une version mettant en évidence les modifications. Selon la nature des modifications, il est recommandé de les discuter au préalable avec la FINMA. 25 4

VII. HISTORIQUE DES AUTORISATIONS

25 5 À ce jour, la FINMA a autorisé **au total 7 établissements fintech**, à savoir Bivial AG (anciennement Klarpay AG), Relio AG, SR Saphirstein AG, Yapea AG, Mogli AG, SWISS4.0 AG et Sequence SA. Actuellement, seuls 5 de ces établissements fintech sont toutefois encore en activité.

25 6 Avec SWISS4.0 AG, un autre établissement fintech agréé a dû être à nouveau **liquidé** en 2025, après Mogli AG en 2022. Selon les informations publiques, la FINMA avait étroitement surveillé SWISS4. 0 AG et exigé très tôt des mesures visant à améliorer la situation financière de la start-up. SWISS4.0 AG et ses organes n'ont pas été en mesure de mettre en œuvre avec succès des mesures appropriées dans un délai raisonnable. Le 4 mars 2025, la FINMA a ouvert la procédure de faillite à l'encontre de cette fintech en raison de craintes fondées de surendettement et de graves problèmes de liquidités. La FINMA a désigné Valfor Avocats Sàrl comme liquidateur judiciaire. SWISS4.0 AG était une « micro » comptant environ 250 clients.

25 7 La surveillance des établissements titulaires d'une autorisation au sens de l'art. 1*b* de la LB s'est également avérée intensive en 2024. La protection des déposants a été au centre des préoccupations en raison de la situation tendue des établissements en matière de fonds propres et de liquidités. Les établissements fintech sont généralement des **start-ups**, qui, comme on peut s'y attendre, engagent des dépenses élevées pour leur mise en place et leur entrée sur le marché et ne disposent au départ que de revenus faibles, voire nuls. Une entrée réussie sur le marché dépend de tours de financement fructueux et d'un modèle économique viable. Jusqu'à présent, les modèles économiques se situent exclusivement dans le domaine des services de paiement. Le marché dans ce secteur est concurrentiel et les marges sont faibles. Il s'est avéré que les modèles économiques ciblant une niche avec une offre unique ou un segment de clientèle spécialisé peuvent être couronnés de succès.

25 8 Le marché des **services de paiement** en Suisse est très concurrentiel et économiquement exigeant. La cessation d'activité n'est pas rare pour les start-ups sur un marché aussi saturé. Cela explique également pourquoi près d'un tiers des entreprises agréées au titre de l'art. 1*b* de la LB ont cessé leurs activités. De plus, contrairement aux clients des banques, les clients des établissements fintech ne bénéficient d'aucune protection des dépôts. Ils ne

bénéficient pas non plus d'un privilège en cas de faillite, bien que les fonds des clients soient détenus dans le bilan de l'établissement. Cela entraîne non seulement des risques de défaillance accrus pour les clients et des défis en matière de surveillance, mais aussi, dans un environnement très concurrentiel, une moindre attractivité de ce type d'autorisation.

C'est notamment dans ce contexte que la **FINMA** exige à juste titre que les établissements de fintech disposent d'une planification continue des fonds propres et des liquidités et soient en mesure d'identifier à temps les goulots d'étranglement. Néanmoins, des situations dangereuses se sont produites en 2024 au sein de plusieurs établissements. La situation s'est souvent aggravée en raison de la valeur douteuse d'actifs dans des *scénarios de « Gone* , lorsqu'une entreprise avait des difficultés à poursuivre ses activités et qu'une liquidation devait être envisagée. Cela concernait notamment l'évaluation des logiciels développés en interne, qui constituent souvent un actif essentiel et qui, sous la pression du temps, peuvent parfois être difficiles à céder. 259

VIII. ÉVOLUTION DE L'AUTORISATION DANS LE DOMAINE DE LA FINTECH

Dans son rapport « Digital Finance : champs d'action 2022+ », dans le champ d'action n° 1, chargé le DFF/SIF, en collaboration avec la FINMA et en concertation avec le secteur, de réexaminer le cadre juridique et prudentiel existant en ce qui concerne les conditions-cadres applicables aux nouveaux acteurs et aux nouvelles formes de services. 260

La FINMA a évalué de manière globalement positive l'autorisation « Fintech dans le cadre de cet examen. Elle a toutefois souligné que l'absence de protection des fonds des clients en cas de faillite constituait un inconvénient majeur de la réglementation actuelle. En raison de cette absence de protection, la surveillance doit répondre à des exigences accrues, d'autant plus que les établissements de ce secteur ne disposent pas d'une situation de rentabilité stable, notamment dans leur phase de démarrage. Une surveillance en temps réel de la situation patrimoniale de l'établissement est donc indispensable. La charge de surveillance de la FINMA pour les établissements fintech est donc disproportionnée par rapport à celle des autres entités surveillées. La FINMA a en outre identifié d'autres faiblesses dans la réglementation actuelle qui compliquent l'activité de surveillance, notamment 261

la possibilité d'un contrôle comptable restreint par la société d'audit (cf. art. 1*b*, al. 4, let. b, LB), les exigences minimales en matière de fonds propres ou l'exercice d'activités accessoires par les établissements fintech.

26 Dans une perspective globale, le Conseil fédéral estime opportun d'intégrer la
2 solution qu'il envisage dans les **travaux de réglementation** correspondants. La solution envisagée prévoit notamment une meilleure protection des dépôts du public en cas de faillite d'un établissement relevant de l'art. 1*b*. Le Conseil fédéral estime à cet égard qu'une adaptation de la réglementation des marchés financiers est nécessaire pour améliorer la protection des clients. L'absence de **protection des clients** ne concerne que les dépôts du public acceptés, et non les actifs cryptographiques (séparables) qui peuvent être acceptés dans le cadre d'une autorisation au titre de l'art. 1*b* de la LB.

Remarque

La présente publication reflète uniquement l'opinion personnelle de ses auteurs et n'engage en rien la FINMA.

Nous remercions chaleureusement le Dr Nico Hess pour la relecture de ce manuscrit.

BIBLIOGRAPHIE

Andreotti Fabio/Zimmermann Stephan/Prantl Florian, Custodial Staking, GesKR 3 (2023), S. 333-354.

Bahar Rashid/Stupp Eric, Kommentierung zu Art. 1 BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Bertschinger Urs, Das Finanzmarktaufsichtsrecht vom vierten Quartal 2017 bis ins vierte Quartal 2018, SZW (2018), S. 708-725.

Bezzola(-Büchler) Dumeng N., Praktische Problemfelder und Lösungsansätze in Bezug auf die «FinTech»-Bewilligungsvoraussetzungen von Art. 1*b* BankG, SZW (2020), S. 534-556.

Bösch René, Kommentierung zu Art. 4^{quater} BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Chapuis Cédric, Kommentierung zu Art. 2 BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Chapuis Cédric, Kommentierung zu Art. 3$^{bis\text{-}ter}$ BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Chapuis Cédric, Kommentierung zu Art. 3^{quater} BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Clemetson Caroline/Etienne Joane, Kommentierung zu Art. 6 FINIG, in: Sethe Rolf/Bösch René/Favre Olivier/Schott Ansgar (Hrsg.), Schulthess Kommentar, Finanzinstitutsgesetz, Zürich 2021.

Frick Thomas/Häusermann Marco, Kommentierung zu Art. 6 FINIG, in: Bahar Rashid/Watter Rolf (Hrsg.), Basler Kommentar Finanzdienstleistungsgesetz/ Finanzinstitutsgesetz, 1. Aufl., Basel 2023.

Hess Nico, Geltungsbereich der bewilligungspflichtigen Tätigkeiten im Bankenrecht de lege lata und de lege ferenda, SSFM 142, Zürich 2023.

Hutzler Doris/Meirich David, Kommentierung zu Art. 2 Abs. 3 GwG, in: Graf Damian K/ Hutzler Doris (Hrsg.), Onlinekommentar zum Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung – Version: 25.01.2026.

Maurenbrecher Benedikt/Kramer Stefan, Kommentierung zu Art. 3*d* BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Meirich David, Regulatorische Einordnung von Decentralized Finance, SSFM 144, Zürich 2023.

Nobel Peter/Brändli Beat/Mächler Monika/Schiltknecht Florian, Schweizerisches Finanzmarktrecht, 5. Aufl., Bern 2026.-

Obrecht Matthias, Fintech-Bewilligung in der Schweiz, Netzwoche vom 10.06.2026, abrufbar unter: https://www.netzwoche.ch/news/2026-06-10/fintech-bewilligung-in-der-schweiz-chancen-huerden-und-erfahrungen, besucht am 12.06.2026 (zit. Obrecht, Netzwoche vom 10.6.2026).

Pfiffner Daniel C., Kommentierung zu Art. 24 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Studer Ueli/Vollenweider Marino, Kommentierung zu Art. 43 FinfraG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Takei Yuto/Shudo Kazuyuki, Pragmatic Analysis of Key Management for Cryptocurrency Custodians, *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dublin 2024, S. 747-765, abrufbar unter: https://takeiyuto.github.io/assets/ckms.pdf (besucht am 12.6.2026).

Winzeler Christoph, Kommentierung zu Art. 3 BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

MATÉRIAUX

Bericht des Bundesrates zu Anpassungen des Bankengesetzes vom 15. Juni 2018, abrufbar unter: https://www.efd.admin.ch/dam/de/sd-web/hcvaF5Xv3zfo/aenderung-bankgesetz-bericht-de.pdf, besucht am 27.4.2026 (zit. Bundesrat, Bericht Bankengesetz).

Bundesrat, Bericht Digital Finance: Handlungsfelder 2022+ vom 1. Februar 2022, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/70095.pdf, besucht am 25.4.2025 (zit. Bundesrat, Bericht Digital Finance).

Bundesrat, Bericht vom 16. Dezember 2022 zu Anpassungen des Bankengesetzes vom 15. Juni 2018, abrufbar unter: https://backend.efd.admin.ch/fileservice/sdweb-docs-prod-efdadminch-files/files/2024/04/30/9fb7f508-2522-428c-a192-23b975c48e93.pdf, besucht am 24.4.2025 (zit. Bundesrat, Bericht 2022).

EFD, Ergebnisbericht des Bundesrates zur Vernehmlassung zur Änderung der BankV FinTech-Bewilligung vom 21. Juni 2018, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/52823.pdf, besucht am 4.4.2025 (zit. EFD, Ergebnisbericht BankV FinTech-Bewilligung 2018).

EFD, Erläuterungsbericht DLT-Verordnung vom 18. Juni 2021, https://www.newsd.admin.ch/newsd/message/attachments/67150.pdf, besucht am 10.4.2025 (zit. EFD, Erläuterungsbericht DLT 2021).

EFD, Erläuterungsbericht DLT-Verordnung zur Vernehmlassungsvorlage vom 22. März 2019, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf, besucht am 10.4.2025 (zit. EFD, Erläuterungsbericht DLT-Verordnung).

EFD, Erläuterungsbericht Revision der Bankenverordnung (BankV) «FinTech-Bewilligung» vom 30. November 2018, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/54881.pdf, besucht am 4.4.2025 (zit. EFD, Erläuterungsbericht BankV 2018).

EFD, Erläuterungsbericht zur Änderung der Bankenverordnung (Fintech) vom 5. Juli 2017, abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/49033.pdf, besucht am 4.4.2025 (zit. EFD, Erläuterungsbericht BankV 2017).

FINMA, Aufsichtsmitteilung 03/2024 - Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen, 7. Juni 2024, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=de&hash=666EEE255C04FB42F01BFD0BC6C80191, besucht am 9.5.2025 (zit. FINMA, Aufsichtsmitteilung 03/2024).

FINMA, Aufsichtsmitteilung 03/2023 – Staking, 20. Dezember 2023, besucht am 23.4.2026, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20231220-finma-aufsichtsmitteilung-08-2023.pdf?sc_lang=de&hash=19EEEFAA320ADED4258F199A8B5C6641 (zit. FINMA, Aufsichtsmitteilung 08/2023).

FINMA, Beurteilung von Bewilligungsprojekten und Vorfragen, abrufbar unter: https://www.finma.ch/de/bewilligung/fintech/fintech-bewilligung/beurteilung-von-bewilligungsprojekten-und-vorfragen/, besucht am 4.4.2025 (zit. FINMA, Beurteilung von Bewilligungsprojekten und Vorfragen).

FINMA, Erläuterungen zu Rundschreiben 2008/21 „Operationelle Risiken – Banken“ – Totalrevision und Rundschreiben 2013/3 „Prüfwesen“ – Teilrevision, 7. Dezember 2022, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/20220510-op-risk-banken/20221213_rs_operat_risiken_anhoerung_eb.pdf?sc_lang=de&hash=050283AF582ECB06D725C6939DCAEC59, besucht am 9.5.2025 (zit. FINMA, Erläuterungen zu RS 2008/21).

FINMA, Fintech Start-up SWISS4.0 SA in Liquidation, Medienmitteilung vom 4. März 2025, abrufbar unter: https://www.finma.ch/de/news/2025/03/20250304-mm-fintech-startup-swiss4_0-liquidation/, besucht am 5.4.2025 (zit. FINMA, Fintech Start-up Swiss4.0 SA in Liquidation).

FINMA, Fintech-Bewilligung, abrufbar unter: https://www.finma.ch/de/bewilligung/fintech/fintech-bewilligung/, besucht am 4.4.2025 (FINMA, Fintech-Bewilligung).

FINMA, Jahresbericht 2018, abrufbar unter: https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20190404-finma-jahresbericht-2018.pdf?sc_lang=de&hash=AAD7EF04090DB3FB5BD0EAF92D8540E0, besucht am 20.4.2026 (zit. FINMA, Jahresbericht 2018).

FINMA, Jahresbericht 2021, abrufbar unter: https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20220405-finma_jahresbericht_2021.pdf, besucht am 10.4.2025 (zit. FINMA, Jahresbericht 2021).

FINMA, Jahresbericht 2024, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20250408-finma_jb24.pdf?sc_lang=de&hash=F5BC9340E3211CAB036BEB2D7A71D2E0, besucht am 10.4.2025 (zit. FINMA, Jahresbericht 2024).

FINMA, Liste der von der FINMA bewilligten Personen nach Art. 1*b* BankG (Fintech-Bewilligung), abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/bewilligungstraeger/pdf/fintech.pdf, besucht am 5.4.2025 (zit. FINMA, Liste der von der FINMA bewilligten Personen nach Art. 1b BankG (Fintech-Bewilligung).

FINMA, Neubewilligung von Banken und Wertpapierhäusern, abrufbar unter: https://www.finma.ch/de/bewilligung/banken-und-wertpapierh%C3%A4user/neubewilligung/, besucht am 28.4.2025 (zit. FINMA, Neubewilligung von Banken und Wertpapierhäusern).

FINMA, Rundschreiben 2017/1, Corporate Governance - Banken, vom 22. September 2016, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/rundschreiben-archiv/2017/rs-17-01/finma-rs-2017-01-20210506_de.pdf?sc_lang=de&hash=7F530363D0237EC203704EFC8E32C624, besucht am 4.4.2025 (zit. FINMA-RS 2017/1).

FINMA, Rundschreiben 2018/3, Outsourcing, vom 21. September 2017, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf, besucht am 4.4.2025 (zit. FINMA-RS 2018/3).

FINMA, Rundschreiben 2023/01, «Operationelle Risiken und Resilienz – Banken», vom 7. Dezember 2022, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf, besucht am 4.4.2025 (zit. FINMA-RS 2023/01).

FINMA, Rundschreiben 2025/4, «Konsolidierte Aufsicht von Finanzgruppen nach BankG und FINIG», vom 1. Juli 2025, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2025-04-20250305.pdf?sc_lang=de&hash=76CE12DBF3489A69BDE38B52875E081F, besucht am 4.4.2025 (zit. FINMA-RS 2025/4).

FINMA, Wegleitung für der FINMA einzureichende Bestätigungen der Prüfgesellschaften zu Gesuchen betreffend die Bewilligung als Personen nach Art. 1*b* BankG („Fintech-Unternehmen“) vom 10. April 2019, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/w_institutsbewilligung-fintech_20190403_de.pdf?sc_lang=de&hash=0571D3925B8E6DA127785B8E1A8DC0BB, besucht am 4.4.2025 (zit. FINMA, Wegleitung für der FINMA einzureichende Bestätigungen der Prüfgesellschaften).

FINMA, Wegleitung für Gesuche betreffend Bewilligung als Person nach Art. 1*b* Bankengesetz (Fintech-Bewilligung) vom 24. April 2025, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/w_bewillligungfintech_20250424.pdf?sc_lang=de&hash=DC7EB79EC1BDFD9E6C31C36306DAFA09, besucht am 4.4.2025 (zit. FINMA, Wegleitung Fintech-Bewilligung).