Partager des valeurs – façonner l'avenir

Regulatory & Compliance Update

Nouvelles réglementations entrées en vigueur et actualité des projets de réglementations dans les domaines bancaire et Asset Management

Septembre 2024

Remarques importantes

La présente publication propose un aperçu des principales réglementations du droit des marchés financiers récemment entrées en vigueur. Elle tient compte du droit international des marchés financiers, respectivement des lois internationales, notamment celles de l'UE, dans la mesure où la commercialisation de produits et de services de la Suisse vers l'étranger implique une obligation de respecter le droit étranger applicable (p. ex. protection des investisseurs). La publication présente également les projets de réglementations pour permettre aux destinataires une planification anticipée des éventuels projets de mise en œuvre des exigences légales ou réglementaires.

Les destinataires de cette publication sont les banques, les maisons de titres, les établissements impliqués dans la gestion d'actifs (direction de fonds, gestionnaire de fortune collective, SICAV, SICAF, SCmPC, autres placements collectifs de capitaux, banque dépositaire de placements collectifs de capitaux, représentant), les gestionnaires de fortune et les trustees.

Etant donné que les modèles d'affaires (prestations de marché) et les orientations territoriales (nationales ou internationales) diffèrent d'un destinataire à un autre, les destinataires ne sont pas tous directement concernés, ni, le cas échéant, dans la même mesure, par ces modifications légales ou réglementaires. Les assurances ne sont pas prises en compte.

Les lois/projets sélectionnés revêtent, de notre point de vue, une importance particulière en raison de leur portée et de leurs répercussions, notamment sur le plan des modifications de processus et des contrôles nécessaires (SCI).

Cette présentation ne se veut pas exhaustive et BDO exclut toute garantie quant à l'exactitude des informations qu'elle contient.

BDO décline toute responsabilité pour les dommages éventuels qui en résulteraient. Les destinataires de cette publication ne sont pas dispensés de l'obligation de se familiariser en détail avec les bases juridiques originales ou les modifications légales et réglementaires. BDO se réserve le droit de procéder à des simplifications quant à la présentation de sa publication.

Sommaire

Nouveautés prévues ou entrées en vigueur

Échange automatique de renseignements (EAR)

Multilateral Competent Authority Agreement (MCAA) et Common Reporting Standard (CRS), comme bases légales internationales (OCDE)

Loi sur l'EAR, Ordonnance sur l'EAR et AFC: «Directive sur la Norme relative à l'échange automatique de renseignements en matière fiscale» (08.01.2021)

Principes de base et nouveautés

- Dans la très grande majorité des cas, la Suisse applique l'EAR sur la base de l'accord multilatéral entre autorités compétentes (Multilateral Competent Authority Agreement; MCAA). Avec l'Union européenne, Hong Kong et Singapour, la Suisse applique l'échange automatique sur la base d'accords bilatéraux.
- La liste de l'ensemble des États et territoires avec lesquels la Suisse entretient des relations d'échanges bilatérales actives se trouve sur le site Internet de l'OCDE. Cette liste comprend les nouveaux États partenaires de la Suisse concernant l'EAR. Elle est tirée de la liste disponible sur le site de l'Administration fédérale des contributions (AFC), laquelle est régulièrement mise à jour et l'emporte sur celle établie par l'OCDE.
- Etats partenaires depuis le 01.01.2024:
  - Thaïlande (juridiction réciproque)
  - Kenya (juridiction réciproque)
- Etats signataires depuis le 01.01.2024:
  - Hong Kong
  - Singapour

  Remarque: lorsque qu'un État se déclare «juridiction non réciproque permanente», il doit livrer des informations sur les comptes financiers aux Etats partenaires, mais n'en reçoit pas de son côté.
- La transmission automatique de renseignements concerne quatre catégories d'institutions financières («institutions déclarantes»): i) les établissements de dépôt, ii) les établissements gérant des dépôts de titres, iii) les entités d'investissement et iv) les organismes d'assurance particuliers.
- Obligations pour les institutions financières suisses déclarantes (chiffres selon directive de l'AFC):
  - Enregistrement auprès de l'AFC (cf. Ch. 10.1)
  - Respect des obligations de diligence raisonnable concernant l'identification de comptes soumis à déclaration (cf. Ch. 6)
  - Obligation d'informer les clients (cf. Ch. 8) et
  - Procédure de déclaration à l'AFC des renseignements à échanger concernant les comptes soumis à déclaration (cf. Ch. 7)

Délais fixés pour la transmission

- Les IF suisses déclarantes transmettent annuellement et de manière électronique les renseignements à l'AFC, au plus tard le 30 juin qui suit l'année civile à laquelle se rattachent les renseignements.

Nouveautés du modèle EAR

- L'échange automatique international de renseignements en matière fiscale doit à l'avenir inclure les crypto-valeurs (communiqué du SFI du 10.11.2023). Dans une déclaration commune, une cinquantaine d'Etats, dont la Suisse, s'engagent aujourd'hui en faveur de l'extension de l'échange automatique international de renseignements en matière fiscale (EAR). L'extension (Crypto-Asset Reporting Framework, CARF) concerne les cryptoactifs et doit s'appliquer à partir du 1er janvier 2026. Le CARF réglemente le traitement des crypto-valeurs et de leurs fournisseurs.

Objectif

- Le CARF doit combler les lacunes du dispositif de transparence fiscale et garantir que les fournisseurs de crypto valeurs soient traités de la même manière que le secteur financier traditionnel. La mise en œuvre du CARF étend la réglementation avancée du marché des cryptomonnaies en Suisse et contribue à la crédibilité et à la réputation de la place financière suisse.

Consultation

- Le Département fédéral des finances (DFF) élaborera d'ici fin juin 2024 un projet de consultation pour la mise en œuvre de l'EAR étendu. La Suisse a l'intention de mettre également en œuvre le CARF.
- L'extension de l'EAR relatifs aux cryptoactifs et la modification de la norme pour l'EAR sur les comptes financiers.
- L'extension comprend également un certain nombre de définitions et de clarifications afin de combler les lacunes et de garantir une applicabilité uniforme des règlements.
- La consultation durera jusqu'au 6 septembre 2024 et devrait entrer en vigueur le 1er janvier 2026.

Mesures à prendre

- Jusqu'au 30 juin 2023: Exécution des devoirs d'annonce à l'attention de tous les États partenaires (y compris la première fois avec les États avec lesquels la Suisse applique l'EAR à partir de janvier 2023)
- Vérification préalable (review) de la base de données des avoirs/comptes financiers concernés (financial assets) en ce qui concerne les mutations pertinentes pour l'EAR (p. ex. départ d'un État tiers) sur la base des États partenaires actuels (voir liste SFI)
- Cadre de contrôle avec vérification des mutations et comparaison avec les paramètres EAR; voir aussi obligation LBA (AML) de vérification périodique de la documentation des clients selon une approche basée sur les risques depuis le 01.01.2023

Calendrier

Nouveaux États partenaires:
1er janvier 2024 (cf. principes de base et nouveautés)

Extension du modèle EAR aux valeurs crypto: dès le 01.01.2026; Elaboration du projet de consultation DFF pour mise en œuvre jusqu'au 15.05.2024.

Banques et maisons de titres: Directement concernés

Asset Management: Indirectement ou partiellement concernés

Gestionnaire de fortune et Trustees: Pas concernés

Protection des investisseurs/ Mesures organisationnelles pour prestataires de services financiers

Loi sur les services financiers (LSFin)

Ordonnance sur les services financiers (OSFin)

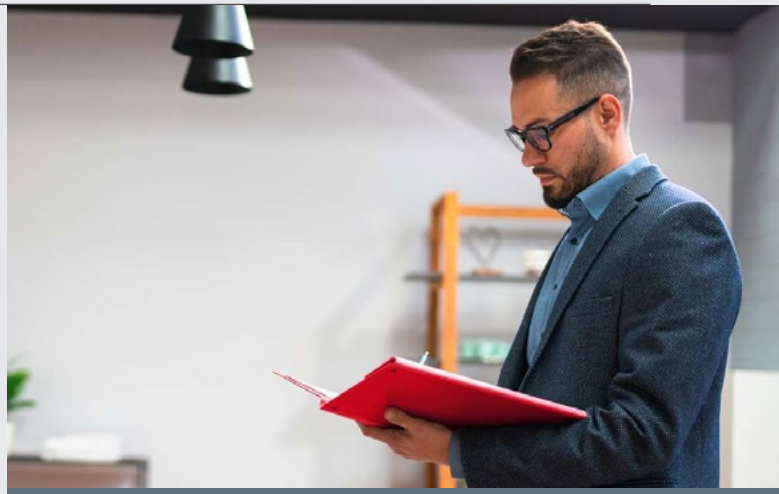
Projet de Circ.-FINMA «Règles de comportement selon la LSFin et l'OSFin» du 15 mai 2024 avec «Rapport explicatif» et «Éléments essentiels»

Principes de base et nouveautés

- La loi sur les services financiers (LSFin) a été créée pour améliorer la protection des investisseurs en renforçant les obligations de diligence et les obligations organisationnelles des prestataires de services financiers et pour combler le fossé en matière de connaissances qu'il y a entre les investisseurs inexpérimentés et les prestataires de services financiers. La LSFin permet d'accorder la législation suisse à la législation européenne (MiFID II/MiFIR, etc.).
- Obligation d'informer les clients avec la conclusion du contrat, respectivement avant l'exécution de l'opération, des coûts et frais ainsi que des conditions spéciales que la banque facture pour ses prestations. Ces informations obligatoires et éventuelles adaptations doivent être communiquées à temps.
- Classification des clients: Subdivision de tous les clients en clients privés, professionnels ou institutionnels.
- Règles de conduite: Examen de l'adéquation («suitability») et du caractère approprié («appropriateness») des produits financiers et des services financiers, en fonction du segment de clientèle et du type de service; le conseil en placement (en tenant compte du portefeuille du client (pas des transactions) ou la mise en œuvre d'un mandat de gestion de fortune nécessite les deux tests précités pour les clients privés: connaissance de la situation financière du client, c.-à-d. revenu et fortune (cf. art. 5 OSFin, comme métaux précieux et assurances vie avec valeur de rachat); y compris les engagements actuels et futurs; en cas de rapports de représentation, le prestataire de services financiers tient compte des connaissances et de l'expérience du représentant (réglementation dans la procuration); exceptions: obligation de vérification en cas d'execution only (indépendamment de la complexité de l'instrument financier) et pour les clients professionnels (y compris les clients privés fortunés selon l'art. 5 LSFin).
- Le prestataire de services financiers peut se fier aux indications données par le client, dans la mesure où il n'y pas d'indices qui laissent penser que cela ne correspond pas à la réalité (cf. art. 17, al. 3, OSFin); le prestataire n'a pas l'obligation de vérifier qu'elles sont plausibles.
- Le prestataire de services financiers note les objectifs de placement en indiquant notamment l'horizon temporel, le but du placement, la capacité de risque et la propension au risque du client et d'éventuelles restrictions de placement (restrictions de titres).
- Le projet de Circ.-FINMA «Règles de comportement selon la LSFin et l'OSFin) précise des exigences en matière de transparence sur:
  - la nature du service financier fourni
  - les risques liés aux instruments ou services financiers
  - la gestion des conflits d'intérêt et la publication des rétrocessions
- La période de consultation s'est achevée le 15 juillet 2024 et l'entrée en vigueur est prévue pour Q1 2025.

Mesures à prendre

- Mise en œuvre de la segmentation des clients sur la base du choix libre du client/information valable au client sur la portée de l'opting-out
- Implémentation dans les formulaires et les systèmes de la vérification de l'adéquation (suitability), respectivement le caractère approprié (appropriateness)
- Mise en œuvre du devoir d'information par le biais de notices et/ou d'un site Internet
- Mise en œuvre des obligations de documentation et de comptes rendus
- Mise en œuvre de l'obligation d'organisation
- Pour les conseillers à la clientèle: obligation de formation et de perfectionnement (garantir les exigences techniques)
- Mise à jour des contrats des gestion et de conseil (obligations d'information étendues selon la Circ.-FINMA)



- Sur la base du projet de Circ.-FINMA Règles de comportement:
  - Adaptation de la documentation ou saisie différenciée dans le système du prestataire de services financiers entre un service de conseil sur portefeuille ou transactionnel
  - Vérification de la transparence envers les clients concernant les produits et services financiers, surtout lorsqu'ils sont très complexes et/ou associés à des risques élevés
  - Vérification de la transparence concernant les conflits d'intérêts, en particulier lors du placement de propres produits du prestataire (le client doit comprendre quand des instruments financiers propres sont choisis par rapport à des instruments tiers)
  - Mise en évidence (également électronique) de l'obtention de rémunérations reçues de tiers et de rétrocessions; revoir le contenu de la renonciation et faire preuve de transparence sur les fourchettes de rémunération pour les différentes classes de produits; et en plus, dans le cas de la gestion de fortune et du conseil en investissement sur portefeuille, sur les fourchettes de rémunération basées sur la valeur du portefeuille et la stratégie d'investissement convenue

Calendrier

Entrée en vigueur: 1er janvier 2025;
Délai de réponse Projet de Circ.-FINMA Règles de comportement LSFin/ OSFin jusqu'au 15 juillet 2024; Évaluation par la FINMA des (nombreuses) réponses; Version finale de la Circ.-FINMA prévue pour Q4 2024

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Etablissements financiers/ Gestionnaires de fortune

Loi sur les établissements financiers (LEFin)
Ordonnance sur les établissements financiers (OEFin)
Ordonnance sur les organismes de surveillance dans la surveillance des marchés financiers (OOS)
Projet d'Ordonnance FINMA sur les établissements financiers (OEFin-FINMA) Demandes LEFin tardives

Principes de base et nouveautés

- L'OEFin concrétise les conditions d'autorisation et les obligations des établissements financiers ainsi que les dispositions liées à leur surveillance.
- L'OS fixe les conditions d'autorisation et les tâches des nouveaux organismes de surveillance.
- L'OEFin-FINMA établit en particulier la démarcation entre les gestionnaires de fortune et les gestionnaires de fortune collective, ainsi qu'entre les exigences en matière d'assurance responsabilité professionnelle, de gestion et de contrôle des risques. L'OEFin-FINMA supprime ainsi plusieurs circulaires FINMA et abaisse le seuil des mesures pour l'identification des clients de CHF 5'000 à CHF 1'000 lors d'opérations de change en cryptomonnaie.
- Concernant les maisons de titres (cf. art. 41 LSFin), et s'agissant des exigences en matière de fonds propres et de liquidité, une nouvelle différenciation est faite entre les établissements avec ou sans gestion de compte.
- Dépôt de la demande auprès de la FINMA, y c. confirmation d'affiliation à un OS, jusqu'au 31.12.2022 = le gestionnaire de fortune peut poursuivre son activité jusqu'à la décision d'obtention de l'autorisation (cf. Communication sur la surveillance, ch. 3.1).

Communication FINMA sur la surveillance 01/2024

- Dans sa communication FINMA sur la surveillance 01/2024, la FINMA informe qu'au 31 décembre 2023 elle avait accédé à 1149 (70%) des demandes d'autorisation de gestionnaires de fortune et des trustees reçues avant le 31 décembre 2022 et que 63 établissements (4%) ont retiré leur demande. Les 487 demandes restantes (26%) sont plus complexes et nécessitent un délai de traitement plus important. Un établissement peut continuer à exercer son activité s'il est encore affilié à un organisme d'autorégulation et qu'il a transmis sa demande d'autorisation à la FINMA avec une preuve de l'assujettissement à un organisme de surveillance (OS) avant la fin du délai transitoire.

Mesures à prendre

- Établissements titulaires d'une autorisation de la FINMA: Satisfaire aux exigences de la LEFin
- Investigations en 2023: Les établissements qui étaient déjà actifs à l'entrée en force de la LEFin et qui n'ont pas déposé de demande auprès de la FINMA à fin 2022 n'ont plus le droit d'exercer leur activité (à titre professionnel) depuis le 1er janvier 2023
- Quiconque exercera intentionnellement ou par négligence sans droit s'exposera aux sanctions prudentielles et pénales évoquées ci-avant (cf. ch. 3.1)
- Conformément à son obligation de procéder à des dénonciations pénales, la FINMA dénoncera ces cas aux autorités de poursuite pénale et engagera de son côté des investigations prudentielles (Communication sur la surveillance, p. 7)

Calendrier

Entrée en vigueur:

- OEFin-FINMA 1er janvier 2021

Banques et maisons de titres: Indirectement ou partiellement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Droit de la SA (CO) Art. 620 ss

(Révision de loi)

Principes de base et nouveautés

Le 1er janvier 2023, la deuxième partie du droit révisé de la société anonyme est entrée en vigueur. A cet égard, les domaines suivants sont concernés par les modifications:

- Structure du capital
  - Le capital-actions, qui s'élève toujours à CHF 100'000 au minimum, peut être fixé dans une monnaie étrangère autorisée comme l'euro, le dollar américain ou la livre sterling, pour autant que ce soit la monnaie courante de l'entreprise (activité commerciale). Un changement de devise est possible au début de chaque exercice.
  - La valeur nominale des actions peut être inférieure à CHF 0,01, mais doit être supérieure à zéro.
  - Introduction d'une marge de fluctuation du capital-actions avec une fourchette de plus ou moins 50% du capitalactions inscrit. Dans le cadre de la marge de fluctuation du capital, le Conseil d'administration peut réduire ou augmenter le capitalactions dans un délai maximal de cinq ans.
  - Suppression des dispositions relatives à la reprise de biens (envisagée) lors de la constitution ou de l'augmentation du capital.
  - Admissibilité de la distribution de dividendes intermédiaires issus de l'activité commerciale courante.
  - Admissibilité du remboursement aux actionnaires de la réserve légale de capital (agio et autres apports supérieurs à la valeur nominale) sous certaines conditions.
- Droits des actionnaires et obligations du Conseil d'administration (CA)
  - Demande de renseignements par les actionnaires dont les actions ne sont pas cotées en bourse et qui disposent d'au moins 10% du capital-actions ou des droits de vote (pas seulement lors de l'AG). Le CA doit fournir les informations dans un délai de quatre mois.
  - Les actionnaires de PME privées qui disposent d'au moins 5% du CA ou des droits de vote ont le droit de consulter les livres de comptes et la correspondance sans autorisation de l'AG, si cela est nécessaire à l'exercice des droits d'actionnaire, sous réserve des intérêts dignes de protection de la société.
  - Abaissement à 5% du seuil des actionnaires minoritaires dans les PME privées pour l'inscription d'objets à l'ordre du jour de l'AG et pour la convocation d'une AG extraordinaire.
  - Le CA doit surveiller en permanence les liquidités de la société. S'il existe une crainte fondée d'insolvabilité imminente, le CA est tenu de prendre des mesures appropriées pour garantir les liquidités et, si nécessaire, d'engager des mesures d'assainissement supplémentaires. Désormais, le CA n'est plus tenu de déposer le bilan auprès du juge des faillites en cas de surendettement s'il existe une perspective fondée que la situation de surendettement puisse se résorber dans un délai raisonnable (au plus tard 90 jours après la présentation des comptes intermédiaires vérifiés). Les créances des créanciers ne doivent pas être mises en péril de manière supplémentaire.
  - L'ancienne disposition relative à la nomination d'un secrétaire du Conseil d'administration a été supprimée. Le procès-verbal peut être signé directement par le rédacteur du procès-verbal au lieu du secrétaire.
- Lieu et mode de tenue de l'Assemblée générale (AG)
  - Convocation d'une AG: peut être demandée par un ou plusieurs actionnaires représentant ensemble au moins 10% du CA; nouveau: extension de ce seuil au nombre de voix (le montant reste toutefois inchangé pour les sociétés non cotées en bourse). Pour les sociétés cotées, un seuil de 5% suffit désormais (cf. art. 699 CO).
  - Droit de proposition et d'inscription à l'ordre du jour: les actionnaires de sociétés cotées en bourse représentant 0,5% du capital-actions ou des voix peuvent demander l'inscription d'un objet à l'ordre du jour; pour toutes les autres sociétés, le seuil est désormais de 5% du CA ou des voix (au lieu d'une valeur nominale de CHF 1 million comme auparavant); (cf. art. 699b CO).
  - Utilisation des technologies numériques lors de la tenue des AG: tenue d'AG virtuelles (par ex. vidéoconférences) (y compris les AG tenues dans différents lieux de réunion ou à l'étranger, pour autant que l'exercice des droits des actionnaires n'en soit pas rendu plus difficile). Les assemblées universelles peuvent désormais être organisées par voie électronique ou sous forme écrite.
- Autres modifications
  - Actions des actionnaires: l'AG peut désormais décider que la société doit intenter une action en restitution ou une action en responsabilité contre un organe fautif tel que le CA ou l'organe de révision. Le délai de prescription relatif pour les actions en responsabilité n'est plus que de trois ans.
  - Enquête spéciale: réduction du seuil pour l'ouverture d'une enquête spéciale (jusqu'à présent: contrôle spécial) par des actionnaires de sociétés ouvertes au public à 5% au moins de l'action ou des voix au lieu de 10% selon l'ancien droit (cf. art. 697d CO).
  - Action en dissolution: un ou plusieurs actionnaires représentant au moins 10% du capital-actions ou des voix peut demander la dissolution pour de justes motifs.

Mesures à prendre

- Adaptation des statuts et des règlements d'organisation
- Les dispositions contraires au nouveau droit des sociétés anonymes restent en vigueur jusqu'au 1er janvier 2025 au plus tard et doivent être modifiées d'ici là
- Les dispositions statutaires conformes au nouveau droit des sociétés anonymes pouvaient déjà être intégrées dans les statuts avant leur entrée en vigueur. Les statuts doivent mentionner que ces nouvelles dispositions n'entreront en vigueur que le 1er janvier 2023
- Recommandation aux PME privées de vérifier les statuts et règlements existants et de décider quand les adapter
- La tenue d'AG virtuelles et d'AG à l'étranger nécessite une base dans les statuts de la société
- Quota de genre de 30% (CA) et 20% (Direction) avec approche «comply or explain» pour les grandes entreprises cotées en bourse, c'est-à-dire les entreprises qui dépassent 2 des seuils de l'art. 727 al. 1 ch. 2 CO (total du bilan de CHF 20 millions, chiffre d'affaires de CHF 40 millions, 250 emplois à plein temps) au cours de 2 exercices consécutifs; en cas de non-respect des valeurs indicatives minimales de l'art. 734f CO, le Conseil d'administration doit, conformément à l'art. 716a al. 1 ch. 8 CO (rapport de rémunération), indiquer les raisons et les mesures prises pour promouvoir le sexe le moins représenté
- Dispositions transitoires concernant le Conseil d'administration au plus tard cinq ans et concernant la Direction au plus tard dix ans après l'entrée en vigueur du nouveau droit, c'est-à-dire à partir du 1er janvier 2026 et du 1er janvier 2031 respectivement

Calendrier

Entrée en vigueur: 1er janvier 2023

Adaptation des statuts au plus tard le 1er janvier 2025

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement/ indirectement concernés

Protection/ Sécurité des données

Principes de base et nouveautés

Objectifs de la protection moderne des données (nLPD/OPDo)

- Protection des personnes physiques lors du traitement de données à caractère personnel (droit fondamental).
- Niveau de protection des données uniforme et élevé pour les personnes physiques en raison de l'évolution rapide des technologies et de la mondialisation («Big Data» comme défi pour la protection des données et le droit de la personnalité; par ex. profilage).
- La protection des personnes physiques devrait être neutre sur le plan technologique et ne pas dépendre des techniques utilisées (data protection by design and by default).

Situation initiale

- La révision totale de la loi sur la protection des données (nLPD) et les dispositions d'exécution contenues dans la nouvelle ordonnance sur la protection des données (OPDo) et la nouvelle ordonnance sur les certifications en matière de protection des données (OCPD) sont entrées en vigueur le 1er septembre 2023.
- La LPD totalement révisée et les dispositions correspondantes dans les ordonnances assureront à l'avenir une meilleure protection des données personnelles pour les personnes physiques (finalité). Elle adapte notamment la protection des données aux évolutions technologiques, renforce l'autodétermination en matière de données personnelles et accroît la transparence lors de la collecte de données personnelles.
- Le Conseil fédéral a adapté le projet de LPD sur plusieurs points:
  - Révision du chapitre sur les obligations des responsables de traitement
  - Exemption des personnes privées de certaines obligations d'information lors de la communication de données personnelles
  - Simplification des modalités relatives au droit d'accès; l'obligation de documenter a notamment été supprimée
  - Adaptation partielle dans le domaine de la sécurité des données (motif: réactions critiques lors de la consultation)
  - Fixation de la durée de conservation des protocoles de traitement des données à au moins un an
  - Insertion d'une nouvelle disposition qui harmonise les objectifs de protection dans le domaine de la sécurité des données avec la nouvelle loi sur la sécurité de l'information du 18 décembre 2020

Principe de base en matière de traitement des données

- Présomption de licéité du traitement des données lorsqu'il est nécessaire à l'exécution ou à la conclusion prévue d'un contrat et que la finalité du traitement est déterminée et reconnaissable par la personne concernée; à des fins de marketing, il faut un consentement [électronique] supplémentaire de la personne concernée par les données.

Application du règlement de base de l'UE sur la protection des données (RGPD)

General Data Protection Regulation (GDPR)

- Le principe du lieu de marché régit et étend le champ d'application géographique du droit européen de la protection des données par les organismes de traitement des données en dehors de l'UE lors du traitement de données à caractère personnel, dans la mesure où l'offre concernée est destinée au marché européen («lieu de marché»).
- Pour les entreprises responsables (contrôleurs), cela a pour conséquence que le RGPD est en principe applicable de par l'orientation vers des marchés cibles dans l'espace de l'UE. En cas de violation des dispositions, les amendes drastiques prévues par le RGPD trouvent donc application (applicables pour tous les États membres de l'UE). La simple mise à disposition du site web, d'une adresse e-mail ou d'autres données de compte ou l'utilisation d'une langue généralement utilisée dans le pays tiers dans lequel le responsable est établi ne suffit pas pour appliquer le principe du lieu de marché; en revanche, toute forme de webtracking (observation, collecte, évaluation du comportement de navigation des personnes physiques concernées sur Internet), ce que l'on appelle le profilage (cf. art. 5, let. f, nLPD ou art. 4, ch. 4, RGPD) suffit aux fins de l'application du principe du lieu de marché.

Droit comparé

- Compatibilité du droit suisse avec le droit européen, notamment avec le règlement général sur la protection des données (RGPD).
- La révision de la LPD doit permettre de maintenir la libre circulation des données avec l'Union européenne afin que les entreprises suisses ne perdent pas en compétitivité (cf. www.kmu.admin.ch).

Mesures à prendre

- Révision des directives et des instructions de travail existantes sur le thème de la protection et de la sécurité des données
- Révision/complément des contrats relatifs à l'externalisation d'activités de traitement à des sous-traitants (Processor) par le responsable (Controller) en ce qui concerne la protection des données personnelles, y compris la sécurité des données (en particulier les solutions Cloud); garantie d'un niveau de protection des données équivalent (norme CH ou UE); cf. art. 9 LPD et art. 7 OLPD
- Vérification des exigences en matière de consentement de la personne concernée en fonction des catégories de données personnelles traitées; en particulier, consentement explicite pour les données personnelles sensibles selon l'art. 5 let. c en relation avec l'art. 6, al. 7, nLPD
- Établissement ou mise à jour d'un registre de protection des données (Records of processing activities/ ROPA) conformément à l'art. 12 nLPD ou à l'art. 30 RGPD; exemption de l'obligation de tenir un registre: entreprises PME et autres organisations de droit privé qui emploient moins de 250 collaborateurs au 1er janvier d'une année, ainsi que les personnes physiques; obligation de ROPA si traitement de données personnelles sensibles à grande échelle ou réalisation de profilage à haut risque
- Garantir un droit d'accès gratuit à la personne concernée dans les 30 jours suivant la demande, conformément à l'art. 25 de la loi révisée sur la protection des données et aux art. 16 ss de l'ordonnance révisée sur la protection des données
- Désigner un responsable de la protection des données (Data Protection Officer/DPO) conformément à l'art. 10 LPD («disposition facultative» pour les responsables privés)
- Recommandation: nomination d'un DPO pour les entreprises de 250 collaborateurs ou plus (interlocuteur direct du Préposé fédéral à la protection des données et à la transparence; surveillance centrale garantie pour la protection des données)
- Analyse d'impact sur la protection des données (Data Protection Impact Assessment/DPIA) en cas de traitement de données présentant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (p. ex. mandat de projet et DPIA comme partie intégrante)
- Formation des collaborateurs à la protection et à la sécurité des données
- Elaboration d'un cadre de contrôle (SCI)
- Réalisation de tests d'intrusion informatique pour combler les failles de sécurité et formations de sensibilisation

Calendrier

Entrée en vigueur:

- nLPD, OPDo et Ordonnance sur les certifications en matière de protection des données (OCPD) 1er septembre 2023

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Lutte contre le blanchiment d'argent

Révision de la LBA et de l'OBA (Conseil fédéral)
Révision de la LBA (entrée en vigueur prévue en 2026)

Principes de base et nouveautés

Aperçu

Avec la révision de la loi sur le blanchiment d'argent (LBA) et de l'ordonnance sur le blanchiment d'argent (OBA), la Suisse améliore son dispositif de défense contre le blanchiment d'argent et le financement du terrorisme (mise en œuvre des recommandations du rapport national du Groupe d'action financière /GAFI).

Les mesures pour les intermédiaires financiers (IF) comprennent:

- Exigences plus strictes en matière d'identification de l'ayant droit économique par l'obligation de vérification des indications relatives à l'ayant droit économique.
- Obligation de vérification et de mise à jour régulière de toutes les relations d'affaires selon une approche basée sur les risques (comportement actif).
- Réglementation relative à la base juridique des communications de soupçons de blanchiment d'argent (cf. art. 9, al. 1quater, LBA, en vigueur depuis le 01.01.2023): soupçon fondé lorsque l'IF dispose d'un signe concret ou de plusieurs indices laissant supposer que les critères de l'al. 1, let. a, pourraient être remplis pour les valeurs patrimoniales impliquées dans la relation d'affaires et que ce soupçon ne peut pas être levé sur la base de clarifications supplémentaires conformément à l'art. 6 LBA.
- Meilleure transparence des associations présentant un risque accru en matière de financement du terrorisme: les associations dont l'activité principale consiste à collecter ou à distribuer directement ou indirectement des fonds à l'étranger à des fins caritatives, religieuses, culturelles, éducatives ou sociales sont tenues de se faire inscrire au registre du commerce (cf. art. 61, al. 2, ch. 3 nCC). Dorénavant, les associations soumises à l'obligation d'inscription doivent tenir une liste de leurs membres et doivent pouvoir être représentées par une personne domiciliée en Suisse et (cf. art. 61a nCC et 69, al. 2 nCC).
- Renforcement de la surveillance et des contrôles dans le domaine des métaux précieux.

Indications pour la pratique:

- Les obligations à respecter en cas de soupçon de blanchiment d'argent ne sont plus fixées dans des ordonnances des autorités de surveillance, mais par le Conseil fédéral lui-même.
- La simple production de copies de pièces d'identité de l'ADE ne remplit plus les exigences en matière de vérification de l'identité: contrôle de plausibilité avec d'autres indications (p. ex. profil KYC, recherches externes) et note au dossier (traçabilité). L'obligation de mise à jour régulière ne constitue pas une nouvelle obligation dans la mesure où, dans la pratique, les IF doivent déjà vérifier périodiquement les données de leurs clients dans le cadre de la catégorisation des risques.
- L'obligation de vérifier périodiquement l'actualité des données relatives aux clients concerne toutes les relations d'affaires, quel que soit le risque. Toutefois, la périodicité et l'étendue de la vérification des indications relative aux clients, se fera sur une approche basée sur les risques. L'approche basée sur les risques est l'émanation d'une réglementation différenciée et proportionnelle. Elle permet aux IF une gestion des risques individualisée, adaptée à leur modèle d'affaires et à leurs types de clients.
- Une dérogation à l'obligation d'inscription au registre du commerce est prévue pour les petites associations. Sous certaines conditions, il sera également possible de renoncer à inscrire au registre du commerce les membres de la direction qui voyagent, afin de les protéger.
  - Voir ci-dessous concernant la communication de la FINMA relative aux exigences en matière d'analyse des risques LBA selon l'art. 25, al. 2, OBA-FINMA.

Révision de la LBA

La révision de la loi sur le blanchiment d'argent (LBA) se concentre principalement sur:

- La création d'un registre de la transparence pour les personnes morales. L'obligation de déclarer les ayants droit économiques au DFJP, qui découle de la création du registre de transparence, incombe aux entreprises concernées. Ces dernières disposent d'un délai d'un mois, après en avoir pris connaissance, pour annoncer les modifications concernant les éléments enregistrés dans le registre. Les infractions aux obligations d'annonce peuvent être sanctionnées par des amendes allant jusqu'à CHF 500'000.
- L'introduction d'obligations de diligence plus étendues pour les conseillers et les avocats.
  La proposition de modification de la loi prévoit que les conseillers et les avocats soient également soumis à la LBA. Cela illustre la volonté de la Suisse de s'adapter à l'évolution des normes mondiales.
- Des mesures supplémentaires de lutte contre le blanchiment d'argent, notamment l'obligation de garantir des mesures organisationnelles afin d'éviter les infractions aux sanctions prévues par la loi sur les embargos (Lemb); abaissement à CHF 15'000 du seuil pour les paiements en espèces dans le commerce des métaux précieux et des pierres précieuses et suppression du seuil pour les obligations de diligence dans le négoce de biens immobiliers
- Entrée en vigueur: Encore incertaine, l'entrée en vigueur des nouvelles dispositions est toutefois prévue pour 2025 ou 2026

Mesures à prendre

- Compléter la directive LBA/FT ou LBA/KYC avec des champs d'action pour la vérification du BO ou du détenteur du contrôle selon la déclaration sur le formulaire A ou K (CDB20) ou les autres formulaires applicables (comparaison avec les données KYC)
- Définir des critères pour la vérification périodique, basée sur les risques, de l'actualité des données des clients et des processus de contrôle (p. ex. relation à risque accru avec vérification annuelle; relation à risque moyen tous les 2-3 ans; relation à faible risque tous les 4-5 ans)
- Lors de l'ouverture de nouvelles relations d'affaires avec des clients organisés sous la forme d'association au sens de l'art. 60 CC, soit les associations disposant de statuts écrits, vérification du but de l'association au regard des exigences de l'art. 61 CC; vérification périodique de la documentation des clients existants organisés sous la forme d'association
- Remarque: les associations au sens de l'art. 61 CC sont considérées comme présentant un risque accru (niveau de risques au sens de de l'OBA-FINMA)

Calendrier

Entrée en vigueur nLBA et OBA: 1er janvier 2023; Le Conseil fédéral a déjà introduit au 1er janvier 2022 une première partie de la révision de la LBA pour les essayeurs du commerce négociant en métaux précieux

Entrée en vigueur des art. 61, al. 2, ch. 3 et art. 61a CC: 1er janvier 2023

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Normes GAFI de lutte contre le blanchiment d'argent

Mise à jour de la liste GAFI de juridictions à hauts risques et sous surveillance

États présentant des lacunes stratégiques en matière de LBA et de FT (modification du Règlement UE et adaptation pour SPG FL)

Principes de base et nouveautés

Situation initiale

- Le Groupe d'action financière sur le blanchiment de capitaux (GAFI) est un organisme international qui a pour objet de concevoir et de promouvoir des stratégies de lutte contre le blanchiment d'argent et le financement du terrorisme et de la prolifération. La Suisse est membre de cette association.
- Jusqu'en octobre 2023, le GAFI a examiné 129 pays et juridictions dont 102 ont été identifiés publiquement. Depuis, 76 d'entre eux ont mis en œuvre les réformes nécessaires pour remédier à leurs faiblesses en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Ils ont donc été retirés du processus. (cf. www.fatf-gafi.org/fr/countries/liste-noire-et-liste-gris.html)

Actifs virtuels (crypto assets)

- Les actifs virtuels présentent de nombreux avantages, mais des dangers également. Ils sont conçus pour faciliter les paiements, rendre les transactions plus rapides et moins couteuses. Ils offrent des méthodes alternatives à ceux qui n'ont pas accès aux produits financiers réguliers. Cependant, en raison de leur manque de réglementation, les actifs virtuels peuvent être plus sujets à la volatilité des prix. De plus, il existe des risques de cyberattaques et de fraude.
- En l'absence d'une réglementation adéquate et pour répondre aux préoccupations liées à l'utilisation abusive des actifs virtuels à des fins criminelles et terroristes, le GAFI, qui a suivi de près les développements dans la cryptosphère, a publié des normes mondiales contraignantes pour le blanchiment d'argent et le financement du terrorisme. (cf. www.fatf-gafi.org/fr/Sujets/actifs-virtuels.html)

Actions pour les intermédiaires utilisant des actifs virtuels

- Les pays doivent tout d'abord terminer la mise en œuvre pleine et efficace des normes du GAFI relatives aux actifs virtuels. Parallèlement, les fournisseurs d'actifs virtuels doivent prendre les mêmes mesures préventives que les établissements financiers, telles que le devoir de diligence envers les clients (CDD), la conservation des documents et la déclaration des transactions suspectes.
- La FINMA a publié à ce sujet les communications suivantes, pertinentes en matière de surveillance :
  - Travel Rule pour les Virtual Asset Service Providers (VASP) 08/2019
  - «Staking» Communication 08/2023 v. 20.12.2023 (avec mention des variantes dans la pratique et des bases pour la conservation)

Juridictions à haut risque (GAFI)

- Les juridictions à haut risque présentent des défaillances stratégiques significatives dans leurs régimes de lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération. Pour tous les pays identifiés comme étant à haut risque, le GAFI en appelle à tous les membres et toutes les juridictions à appliquer des mesures de vigilance particulières et, dans les cas les plus sérieux, les pays sont appelés à appliquer des contre-mesures afin de protéger le système financier international face aux risques existants de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération liés au pays. Cette liste est souvent appelée la «liste noire» (https://www.fatf-gafi.org/fr/countries/black-and-grey-lists.html)
- Juridictions à haut risque: République démocratique et populaire de Corée, Iran et Myanmar.

Juridictions soumises à une surveillance accrue

- Les juridictions soumises à une surveillance accrue travaillent activement avec le GAFI pour remédier aux défaillances stratégiques de leurs régimes de lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération. Lorsque le GAFI place une juridiction sous surveillance accrue, cela signifie que le pays s'est engagé à remédier rapidement à la défaillance stratégique identifiée, dans le délai convenu, et qu'il est soumis à une surveillance accrue. Dans les milieux externes au GAFI, cette liste est souvent appelée «liste grise».

Juridictions de la «liste grise» (Etat au 23.02.2024):

- Afrique du Sud, Bulgarie, Burkina Faso, Cameroun, Croatie, Haïti, Kenya, Mali, Monaco, Mozambique, Namibie, Niger, Philippines, République Démocratique du Congo, Sénégal, Soudan du Sud, Syrie, Tanzanie, Venezuela, Vietnam, Yémen

Juridictions qui présentent des défaillances stratégiques

- Selon le projet de règlement délégué (UE) 2023/2070 de la Commission du 18 août 2023, il est nécessaire de modifier le règlement délégué (UE) 2016/1675. Celui-ci est directement déterminant pour les obligations selon l'art. 11a de la loi liechtensteinoise sur l'obligation de diligence concernant les juridictions qui présentent des défaillances stratégiques. Dans le cadre de la communication de la FINMA concernant les exigences relatives à l'analyse du risque LBA selon l'art. 25 al. 2 OBA-FINMA, une modification de la classification en pays à risque par des Etats étrangers augmente également pour les banques suisses et les autres intermédiaires financiers la classification du risque par rapport aux clients ou aux ayants droit économiques qui ont leur domicile/siège dans ces pays.

Juridictions à risques élevés (état au 02.07.2024)

- Afghanistan, Bosnie-Herzégovine, Guyana, Irak, Iran, Ouganda, République populaire démocratique de Corée, Syrie, Vanuatu, Yémen

Mesures à prendre

- Revue et le cas échéant correction du niveau de risque des relations d'affaires impactées par les critères de risques de l'art. 13, al. 2 et 3 let. d OBA-FINMA, qui renvoie à la liste des pays que le GAFI considère à haut risque ou non coopératif (nationalité du cocontractant ou de l'ayant droit économique des valeurs patrimoniales ou type et lieu de l'activité commerciale du cocontractant ou de l'ayant droit économique des valeurs patrimoniales ou pays d'origine ou de destination de paiements fréquents)
- Attribution du niveau de risque de la juridiction déterminante pour la classification des risques et la mise à jour périodique de la documentation du client (annuellement pour les clients à haut risque); y compris le monitoring des transactions LBA

Calendrier

Publication: Novembre 2023

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Sanctions SECO, UE et OFAC/ Sanctions du Conseil fédéral à l'encontre de la Russie

Principes de base et nouveautés

Situation initiale

- Le 28 février 2022, le Conseil fédéral a décidé de reprendre les sanctions de l'UE contre la Russie. L'ordonnance suisse a donc fait l'objet d'une révision totale le 4 mars 2022.
- Pour les banques, les articles 20 et 21 de l'ordonnance sont à souligner:
  - Interdiction d'accepter des dépôts de plus de CHF 100'000 de ressortissants russes ou de personnes physiques/entités établies en Russie (art. 20; avec des dispositions d'exception pour les ressortissants suisses, les ressortissants d'un État membre de l'UE et les personnes physiques titulaires d'un titre de séjour temporaire ou permanent de la Suisse ou d'un État membre de l'UE).
  - Obligation de déclarer au SECO, d'ici au 3 juin 2022, les dépôts existants de plus de CHF 100'000 de ressortissants russes ou de personnes physiques/ entités établies en Russie (art. 21). Le 16 mars 2022, le SECO a publié une interprétation de ces articles d'ordonnance (en lien sous «Informations complémentaires»).

Mise à jour des sanctions du 31.01.2024 (CF):

- Le 28 février 2022, le Conseil fédéral a décidé de reprendre les sanctions de l'Union européenne (UE) contre la Russie et de renforcer leurs effets. L'ordonnance actuelle a donc fait l'objet d'une révision totale le 4 mars 2022.
- Les mesures comprennent notamment des interdictions concernant les biens à double usage, les biens militaires spécifiques et les biens destinés au renforcement militaire et technologique ou au développement du secteur de la défense et de la sécurité, et l'interdiction d'émettre et de négocier des valeurs mobilières et des instruments du marché monétaire..
- Le Conseil fédéral a modifié et renforcé l'ordonnance du 31.01.2024 sur les mesures en rapport avec la situation en Ukraine. Il s'agit notamment de mettre en œuvre et de faire respecter les sanctions prononcées et de lutter contre tout contournement.
- Des modifications sont régulièrement publiées et peuvent être consultées sur: https://www.seco.admin.ch/seco/fr/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen/massnahmen-zur-vermeidung-der-umgehung-internationaler-sanktione.html

Mesures à prendre

- Les banques doivent s'assurer qu'elles n'acceptent pas de dépôts supérieurs à CHF 100'000 de la part de citoyens russes ou des personnes physiques/entités établies en Russie (par client; en tenant compte de la disposition d'exception)
- Vérifier quels clients sont des citoyens russes ou des personnes/ entités établies en Russie
- Déclarer au SECO les dépôts de citoyens russes et de personnes/ entreprises domiciliées en Russie
- Les intermédiaires financiers sont tenus, conformément aux dispositions de l'ordonnance, de mettre en œuvre les interdictions, de procéder au gel des valeurs patrimoniales des personnes sanctionnées et d'annoncer les relations d'affaires concernées au SECO
- L'annonce faite au SECO ne dispense pas les intermédiaires financiers, de procéder, en cas de soupçons, à des clarifications supplémentaires au sens de l'art. 6 LBA et, lorsqu'ils ne sont pas en mesure de les écarter, d'effectuer immédiatement une communication au sens de l'article 9 LBA au Bureau de communication en matière de blanchiment d'argent

Calendrier

Entrée en vigueur: surveillance constante et mise à jour des listes de sanctions

Banques et maisons de titres: Directement concernés

Asset Management: Indirectement ou partiellement concernés

Gestionnaire de fortune et Trustees: Indirectement ou partiellement concernés

Analyse des risques de blanchiment d'argent

Communication FINMA sur la surveillance 05/2023
Analyse des risques de blanchiment d'argent au sens de l'art. 25, al. 2 OBA-FINMA

Principes de base et nouveautés

Aperçu de la Communication FINMA sur la surveillance et points pertinents

- Lors de la mise en œuvre pratique selon l'art. 25, al. 2, OBA-FINMA, les banques sont tenues d'établir une analyse des risques de blanchiment d'argent en tenant compte de son domaine d'activité et de la nature des relations d'affaires gérées. Sur la base de cette analyse, les banques doivent en outre déterminer pour chacun des critères mentionnés à l'art. 13, al. 2, OBA-FINMA s'il est pertinent pour leurs activités, et également établir périodiquement une analyse des risques sur une base consolidée (cf. art. 6, al. 1, let. a, OBA-FINMA). L'obligation de déterminer, de limiter et de contrôler les risques découle également pour les banques des exigences organisationnelles. Des explications détaillées à ce sujet se trouvent dans la circulaire FINMA 2017/1 «Gouvernance d'entreprise – banques».

Contenu

- Exigences plus strictes pour les analyses des risques des banques
- Exigence d'une définition adéquate de la tolérance au risque de blanchiment d'argent avec prise en compte de limites fixées
- Renforcement des éléments structurels (p. ex. segments de clientèle, domicile, forme du produit, champ d'action géographique, etc.) comme condition de base d'une analyse efficace des risques

Tolérance au risque de blanchiment d'argent

Les principes de gestion des risques, ainsi que les compétences et les procédures correspondantes doivent être définies dans un règlement ou des directives internes appropriés (cf. art. 19 OBA-FINMA).

- La définition de la tolérance au risque doit prévoir l'exclusion délibérée de certains pays, segments de clientèle, services et/ou produits afin de présenter une adéquation suffisante
- Les processus pour les exceptions à la tolérance au risque définie (processus «exception to policy») doivent faire l'objet d'une directive, être approuvés par la Direction et surveillés par l'organe de direction suprême
- Les indicateurs de risque clés pour la surveillance de la tolérance au risque doivent être définis avec suffisamment de précision pour permettre à la Direction et au Conseil d'administration d'effectuer des contrôles réguliers

Analyse des risques de blanchiment d'argent

L'analyse des risques doit permettre d'identifier, enregistrer, analyser et évaluer tous les risques de blanchiment d'argent auxquels l'intermédiaire financier est exposé. Sur la base de ces conclusions, il définit ses mesures de gestion, de pilotage, de contrôle, de reporting et de surveillance des risques (cf. rapport explicatif sur la révision partielle de l'OBA-FINMA du 11 février 2015).

- Les paramètres obligatoires pour déterminer le risque global sont notamment:
  - Le siège ou le domicile du client,
  - Le segment de clientèle,
  - Les produits et services proposés,
  - La présence géographique de l'établissement,
  - Ainsi que d'autres catégories qui sont à déterminer individuellement en fonction du modèle d'affaires de chaque banque.
- Les points suivants doivent être vérifiés et, le cas échéant, adaptés :
  - Le risque de blanchiment d'argent doit être déterminé individuellement et de manière compréhensible pour chaque catégorie de risque en ce qui concerne le risque inhérent, le risque de contrôle ainsi que le risque net qui en résulte.
  - Les mesures ayant pour effet de réduire les risques inhérents (risque de contrôle) doivent être décrites de manière suffisamment détaillée en tenant compte d'indicateurs chiffrés.
  - Évaluation de la pertinence des différents critères dans l'analyse des risques, présentée de manière compréhensible pour des tiers.
  - Définition d'indicateurs chiffrés permettant de déterminer l'importance de chaque exposition au risque dans l'ensemble de la clientèle et prise des mesures correspondantes (p. ex. renforcement de la conformité, adaptation de la politique de risque, etc.)

Mesures à prendre

Nécessité éventuelle d'agir

Afin de répondre aux exigences de la FINMA, il convient d'accorder une attention particulière aux points suivants lors de la mise en œuvre pratique et, le cas échéant, de prendre des mesures appropriées.

- Analyser des risques en trois catégories: risque inhérent, risque de contrôle et risque net avec évaluation des risques distincte
- Vérifier les paramètres pour déterminer le risque global (en fonction du modèle d'affaires)
- Étayer les mesures visant à réduire les risques inhérents par des chiffres clés et des critères d'efficacité, en plus de la description.
- Effectuer un examen périodique des paramètres et des catégories de risque et documenter les processus d'audit
- Soumettre l'analyse des risques LBA à la direction et obtenir son approbation (procès-verbal).

Calendrier

Publication: 24 août 2023

Banques et maisons de titres: Directement concernés

Asset Management: Indirectement ou partiellement concernés

Gestionnaire de fortune et Trustees: Indirectement ou partiellement concernés

Communication FINMA 08/2023

Staking

Principes de base et nouveautés

Contenu

- Le «staking» et les exigences associées de la loi sur la technologie des registres électroniques distribués (BBl 2020 7801 Loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués) sont récemment devenus un segment croissant du marché financier. La Communication FINMA sur la surveillance 08/2023 aborde et clarifie les questions pertinentes.

Définitions des termes

- Staking = Le processus de blocage de cryptoactifs natifs sur l'adresse «staking» d'un nœud de validation pour participer au processus de validation d'une blockchain basée sur un mécanisme de consensus de preuve d'enjeu.
- Les participants reçoivent des staking rewards en récompense du staking de cryptoactifs.
- Mécanisme de preuve d'enjeu = processus de validation de transactions individuelles (blocs) dans la chaîne de blocs par un tirage aléatoire d'un participant, la probabilité du tirage augmentant pour les utilisateurs dont le nombre de jetons attribués au nœud de validation est élevé.
- Node = On désigne par «noeud» tout ordinateur qui se connecte à la cryptomonnaie correspondante de son choix via le téléchargement du logiciel open source. Il sert en principe de point de connexion pour les transmissions de données en interaction avec d'autres participants (nœuds) du réseau dans le monde entier, qui forment au total l'épine dorsale de la blockchain.

Risques de l'empilage

- Risques techniques et pénalités
  Lors du processus, des problèmes de système ou de connexion (p. ex. interruption de la connexion Internet) peuvent survenir, ce qui peut entraîner une interruption du mécanisme. Il existe ainsi un risque de slashing des cryptoactifs. Ainsi les cryptoactifs stakés sont entièrement ou partiellement détruits en raison du comportement problématique du validateur.
- Risque de faillite de la contrepartie
  Jusqu'à présent, la situation juridique concernant le traitement des cryptoactifs stakés en cas de faillite de la contrepartie n'est pas claire. Le risque correspondant est considérablement accru lorsque la conservation ou le staking est assuré par des établissements ayant leur siège à l'étranger.
- Risques de marché
  Les cryptoactifs stakés peuvent être retardés dans leur rachat par une période de lock-up/exit dans le cadre du processus d'unstaking. Dans une phase volatile, le détenteur peut ainsi ne pas être en mesure de vendre les valeurs au bon moment. Ces phases peuvent en outre être prolongées pour certaines blockchains (p. ex. Ethereum), la période de lock-up s'allongeant avec l'augmentation du nombre d'ordres unstaking.

Traitement prudentiel

- Traitement en droit de la faillite (art. 242a al. 2 LP)
  La protection contre la faillite des cryptoactifs utilisés pour le staking n'existe donc pas si le dépositaire effectue le staking pour son propre compte, c'est-à-dire s'il effectue une opération pour son propre compte selon l'art. 1a let. b LB. L'exécution du staking par un tiers sur ordre et pour le compte du propriétaire s'avère toutefois plus difficile. Dans ce cas, il faut procéder à une évaluation au cas par cas du mécanisme spécifique de staking. Les mécanismes qui ne prescrivent pas de période de verrouillage ne posent pas de problème, car dans ce cas, les cryptoactifs stakés sont à tout moment à la disposition du propriétaire.
- Traitement en droit bancaire (art. 1a et 1b LB en relation avec les art. 5 et 5a OB)
  Il convient de noter ici que le dépôt individuel est qualifié d'activité d'intermédiaire financier couverte par la LBA et que les prestataires de services correspondants doivent s'affilier à la surveillance en matière de blanchiment d'argent d'un organisme d'autorégulation.
- Enregistrement comptable et exigences prudentielles
  Dans le cas d'une chaîne de stacking, les cryptoactifs stakés sont transmis par le prestataire de services avec la relation client à un ou plusieurs tiers qui exploitent le Validator Node (Noeud de validation) et qui disposent des Withdrawal Keys (retraits clés). Si un établissement autorisé délègue l'exploitation à un tiers, il a une créance envers ce dernier sur le plan comptable, qui peut être comptabilisée soit comme une créance envers le tiers, soit comme une valeur de dépôt au sens d'une créance conservée à titre fiduciaire (art. 16, ch. 2, LB). Cela présuppose une application par analogie des directives de SwissBanking concernant les placements fiduciaires adaptée aux risques des cryptoactifs. Dans le cas du direct staking, le prestataire de services exploite lui-même le Validator Node ou en délègue l'exploitation à un prestataire technique, mais conserve au moins lui-même les Withdrawal Keys pour la reprise des valeurs patrimoniales cryptographiques stackées du client. Une séparation au sens de l'art. 16, ch. 2, LB ne s'applique donc pas.

Mesures à prendre

- Assurer une instruction claire du client de staking en incluant les cryptoactifs nécessaires au staking et une information transparente sur toutes les opportunités et les risques.
- Examen permanent des risques opérationnels (conception dans la gestion de la continuité des activités) des services de staking et adaptation si nécessaire.

Calendrier

Publiée le 20 décembre 2023

Banques et maisons de titres Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Révision OPP 3

Rachats ultérieur dans le pilier 3a

Principes de base et nouveautés

Contenu

- Le 22 novembre 2023, le Conseil fédéral a soumis en consultation la révision de l'ordonnance sur les déductions admises fiscalement pour les cotisations versées à des formes reconnues de prévoyance professionnelle (OPP 3) en vue d'introduire des rachats dans le pilier 3a. A l'avenir, les lacunes de cotisations dans le pilier 3a pourront être comblées ultérieurement, dans un délai de 10 ans maximum, par des rachats fiscalement déductibles. Cette mesure vise à renforcer la prévoyance individuelle fiscalement avantageuse et à apporter un soutien supplémentaire au système suisse de sécurité sociale.

Les principales nouveautés de l'art. 7a OPP 3

- Les cotisations déductibles dans le pilier 3a selon l'art. 7 OPP 3 peuvent désormais également être versées sous forme de rachats. Toute personne disposant d'un revenu soumis à l'AVS en Suisse et ayant donc le droit de verser une contribution à la prévoyance individuelle liée au cours de l'année de rachat a le droit d'effectuer un rachat. Il faut en outre que l'ayant droit n'ait pas épuisé le cadre maximal autorisé au cours des dix années absolues précédant l'année de rachat. Les lacunes de cotisation qui remontent à plus longtemps ne peuvent plus être comblées.
- Les lacunes ne peuvent être comblées que pour les années de cotisation au cours desquelles le preneur de prévoyance a également rempli les conditions pour le versement de cotisations du pilier 3a. Le potentiel de rachat résulte de la somme des lacunes de cotisation des dix dernières années donnant droit à une compensation ultérieure. Dans ce contexte, le montant maximal doit être calculé séparément pour chaque année de cotisation, déduction faite des cotisations versées.
- Les rachats sont possibles en cumulant les cotisations annuelles maximales autorisées et supposent en même temps que les preneurs de prévoyance les ont épuisées au cours de l'année où le rachat doit être effectué. Ainsi, selon l'art. 7a, al. 1, let. c, OPP 3, un rachat ne peut pas être effectué à la place de la cotisation ordinaire.
- Les rachats sont possibles chaque année et donc dans n'importe quelle année de cotisation, à condition que les exigences de l'art. 7 OPP 3 soient remplies.
- Selon l'art. 7a al. 2 OPP 3, le versement de rachat peut s'élever au maximum à 8 pour cent du montant limite supérieur de CHF 88 200 selon l'art. 8 al. 1 LPP et est ainsi limité au montant de la déduction selon l'art. 7 al. 1 let. a OPP 3.
- En outre, la lacune de cotisation d'une année de cotisation ne peut être comblée que par un seul rachat. Il n'est donc pas possible d'effectuer plusieurs rachats annuels pour combler une seule lacune.
- En outre, le droit au rachat suppose qu'aucun versement de la prestation de vieillesse selon l'art. 3 al. 1 OPP 3 n'a encore eu lieu. Le preneur de prévoyance perd donc la possibilité d'effectuer un rachat ultérieur dans le pilier 3a dès qu'il perçoit la prestation de vieillesse. En revanche, un rachat reste possible dans les 5 ans suivant l'âge ordinaire de la retraite, à condition que le preneur de prévoyance continue à travailler.

Conditions en résumé

- Le droit aux cotisations de l'année de rachat a été épuisé au maximum
- La lacune de cotisation envisagée ne remonte pas à plus de 10 ans
- Le droit aux contributions pour l'année de la lacune existait et n'a pas été entièrement utilisé
- Le versement de rachat ne dépasse pas CHF 7065
- La lacune de cotisation de l'année de cotisation spécifique n'a pas déjà été partiellement comblée par un versement de rachat de l'année précédente
- Pas encore de perception de la rente AVS

Exécution du rachat

Un rachat doit être demandé par écrit à l'institution de prévoyance et examiné par celle-ci. La demande doit contenir les éléments suivants:

- Confirmation que la cotisation ordinaire a été entièrement versée au cours de l'année de cotisation actuelle;
- Confirmation que la lacune de cotisation de l'année spécifique n'a pas déjà été comblée par des rachats d'années précédentes;
- Confirmation des preneurs de prévoyance qui ont atteint l'âge de 60 ans qu'aucune prestation de vieillesse n'a été perçue jusqu'à présent.

Conséquences fiscales

- L'Administration fédérale des contributions part du principe que les pertes de recettes annuelles estimées pour l'impôt sur le revenu des cantons et des communes s'élèveront en gros à CHF 200-450 millions et à CHF 100-150 millions pour l'impôt fédéral direct

Calendrier

Entrée en vigueur: 1er janvier 2025

Banques et maisons de titres: Indirectement ou partiellement concernés

Asset Management: Indirectement ou partiellement concernés

Gestionnaire de fortune et TrusteesIndirectement ou partiellement concernés

Actualité des projets de réglementations

Rapport sur les questions climatiques en Suisse

L'ordonnance d'exécution du Conseil fédéral relative au rapport sur les questions climatiques du 23 novembre 2022

DFJP 26.06.2024: Modification du Code des obligations (transparence sur les questions de durabilité)

Rapport explicatif relatif à l'ouverture de la procédure de consultation

ASB Mai 2024: Modification de la directive actuelle Environmental, Social and Governance (ESG)

Principes de base et nouveautés

Communication FINMA sur la surveillance 01/2023: Évolutions concernant la gestion des risques climatiques (24.01.2023)

- Dans cette communication, la FINMA attire notre attention sur les évolutions internationales importantes dans le domaine de la gestion des risques financiers liés au climat. Elle réaffirme qu'elle attend des établissements soumis à sa surveillance qu'ils identifient et gèrent de manière appropriée les risques climatiques sur la base de procédures reconnues. En particulier, ceux-ci doivent étudier activement les recommandations et pratiques établies par les organismes internationaux pertinents tels que le Network for Greening the Financial System (NGFS) ou l'AICA.
- Dans ce cadre, les organismes internationaux de normalisation élaborent des recommandations et des aides concrètes pour la gestion des risques climatiques et attendent des banques et des entreprises d'assurance qu'elles gèrent efficacement les risques climatiques à l'instar de tout autre risque, y compris en matière de gouvernance, gestion des risques ou de publication.

DFJP - Modification du CO:

Contenu de la procédure de consultation:

- Le champ d'application du règlement sera élargi par l'abaissement du seuil des «emplois à temps plein» de 500 à 250. Il suffira désormais que deux des trois seuils (équivalents temps plein, chiffre d'affaires et total du bilan) soient atteints au cours de deux exercices consécutifs. La possibilité de pouvoir se dispenser du reporting est éliminée (approche «comply or explain»). Le champ d'application des informations sur les aspects liés à la durabilité sera élargi et précisé. Contrairement aux entreprises de l'UE, les entreprises suisses devraient avoir le choix d'orienter leur rapport sur la durabilité soit sur la norme de l'UE, soit sur une autre norme équivalente. Le Conseil fédéral fixe ces normes dans une ordonnance.
- La loi sur la surveillance de la révision (LSR) précise également de nouvelles dispositions.

Nouvelle circulaire FINMA sur les risques climatiques et autres risques naturels

- La FINMA élabore actuellement une nouvelle circulaire intitulée «Risques financiers liés à la nature», qui s'appliquera aux banques et aux assurances. La FINMA entend ainsi préciser les exigences relatives à la gestion des risques des établissements en ce qui concerne les risques climatiques et les autres risques financiers liés à la nature. La circulaire intégrera les recommandations actuelles des organismes de normalisation internationaux, en particulier le CBCB et l'AICA, ainsi que certaines des recommandations du NGFS (Q1 2024: La FINMA lance la première audition publique). La FINMA met ainsi en œuvre les recommandations pertinentes du Network for Greening the Financial System (NGFS).
- Ordonnance d'exécution du Conseil fédéral relative au rapport sur les questions climatiques: Les sociétés ouvertes au public, les banques et les assurances comptant 500 employés ou plus, dont le total du bilan est égal ou supérieur à CHF 20 millions et le chiffre d'affaires dépasse CHF 40 millions devront publier un rapport sur les questions climatiques selon les recommandations de la TCFD.
- Les recommandations de la TCFD sont considérées comme une norme internationale reconnue. La mise en œuvre des recommandations du TCFD doit également tenir compte des recommandations intersectorielles ainsi que des orientations spécifiques à certains secteurs. La mise en œuvre est un processus itératif.
- Le rapport sur les questions climatiques établi sur la base des recommandations TCFD doit appréhender 4 thèmes: i) gouvernance; ii) stratégie; iii) gestion des risques et iv) indicateurs et objectifs.
- Directives de l'Association suisse des banquiers («ASB») de juin 2022 pour ses établissements membres:
  - Directives pour les prestataires de services financiers relatives à l'intégration des préférences ESG et des risques ESG dans le conseil en placement et la gestion de fortune»; mai 2024: Directives pour les prestataires de services financiers relatives à l'intégration des préférences ESG et des risques ESG, et à la prévention de l'écoblanchiment dans le conseil en placement et la gestion de fortune; Les exigences de ces directives entreront en vigueur le 01.09.2024.
  - Document Q&A (Conseil en placement et Gestion de fortune) concernant les directives du 12.01.2023
  - «Directives pour les fournisseurs d'hypothèques relatives à l'amélioration de l'efficacité énergétique des bâtiments»
- Les critères ESG consistent en un ensemble de normes environnementales, sociales et de gouvernance applicables aux activités des entreprises. Ces critères s'inscrivent, au sens large, dans la responsabilité sociale des entreprises (RSE), qui permet de mesurer les effets des activités des entreprises sur la société et l'environnement, en prenant notamment en compte: La contribution des entreprises au développement durable et les conditions de travail (y compris la protection de la santé), les droits de l'homme, l'environnement, la prévention de la corruption, la concurrence équitable, les intérêts des consommateurs, la fiscalité et la transparence.
- ESG est, entre autres, un paquet réglementaire européen d'envergure, qui tend à définir le cadre et la gestion des investissements durables.
  - Règlement 2020/852 établissant un cadre visant à faciliter les investissements durables (appelé «taxonomie»): établit les critères permettant de déterminer si une activité économique peut être considérée comme durable sur le plan environnemental
  - Règlement 2019/2088 sur la publication d'informations en matière de durabilité dans le secteur des services financiers («SFDR»), obligeant les institutions financières de l'UE à respecter différentes obligations de publication
  - Règlement sur les valeurs de référence pour les investissements à faible émission de carbone et les investissements à bilan carbone favorable, dans le but de créer des normes pour les indices de référence à faible émission de carbone et à impact carbone positif
  - MiFID II: impose aux établissements financiers de prendre en considération les préférences ESG des investisseurs dans la définition de leurs questionnaires d'adéquation (suitability assessment) qu'ils proposent aux clients.

Mesures à prendre

- Mise en place d'une gestion des risques climatiques adéquate et correspondant au profil de risque des clients
- Prendre en compte de manière proactive les recommandations émises par les organismes internationaux ainsi que les bonnes pratiques du marché
- Développement des processus internes (notamment de contrôle) pour les établissements soumis à la surveillance de la FINMA
- Révision de la stratégie et de la planification de l'entreprise (les enjeux climatiques comme composante stratégique)
- Analyse de la gouvernance de l'entreprise par rapport aux exigences de l'ordonnance du CF et aux critères ESG: principe top-down
- Définition d'un mandat de projet «TCFD» (obligatoire pour toutes les unités organisationnelles) avec identification et analyse préalable des irrégularités par rapport aux recommandations TCFD
- Plan d'action avec définition des tâches, des objectifs et des responsabilités
- Analyse des produits d'investissement/financiers avec accent sur les normes RSE
- Formation des collaborateurs aux critères ESG et aux normes RSE et introduction de facteurs de motivation (partie intégrante de la convention d'objectifs)
- Communication pour les clients et les autres parties prenantes
- Intégration des risques de durabilité dans la gestion interne des risques

Calendrier

Entrée en vigueur:

- Ordonnance du CF le 1er janvier 2024
- Publication du premier rapport sur le climat après l'ordonnance du CF d'ici fin 2024
- Règlements européens: Entre 2020 et 2022
- Entrée en vigueur des directives de l'ASB pour les établissements membres: 1er janvier 2023

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Indirectement ou partiellement concernés

Création d'un registre de transparence pour les ayants droit économiques

Principes de base et nouveautés

Mandat du Conseil fédéral

- Lors de sa séance du 12 octobre 2022, le Conseil fédéral a chargé le Département fédéral des finances (DFF) d'élaborer, d'ici au deuxième trimestre 2023, un projet de loi visant à accroître la transparence et à faciliter l'identification des ayants droit économiques des personnes morales. Il entend ainsi renforcer la prévention et la poursuite pénale dans le domaine de la criminalité financière et, par conséquent, l'intégrité et la réputation de la place financière suisse.
- Le 30 août 2023, le projet de «Loi fédérale sur la transparence des personnes morales et l'identification des ayants droit économiques» a été mis en consultation. L'objectif est de présenter un message au Parlement en 2024.
- Base légale actuelle aux art. 697j ss. CO («Répertoire des ayants droit économiques»); inséré selon la Loi Fédérale du 12 décembre 2014 sur la mise en œuvre des recommandations du Groupe d'action financière (GAFI/ FATF) révisées en 2012.
- But: augmenter la transparence pour faciliter l'identification des ayants droit économiques des personnes morales.
- Résultat: la mise en œuvre des exigences légales actuelles est insuffisante.

Objectif

- Accroître la transparence pour faciliter l'identification des ayants droit économiques des personnes morales. Le projet vise notamment à introduire un registre central d'identification des ayants droit économiques et de nouvelles obligations de maintien à jour des informations sur les ayants droit effectifs en fonction des risques.
- Le registre doit être accessible aux autorités compétentes, mais pas au public.
- Le Conseil fédéral attache la plus grande importance à la lutte contre la criminalité financière et franchit, avec ce projet, une nouvelle étape dans le renforcement du dispositif suisse. En même temps, il concrétise sa stratégie 2021-2024 contre la corruption.
- En plus du niveau national, la Suisse a participé à la mise en place d'un système mondial d'identification des acteurs des marchés financiers (GLEIF) afin d'améliorer la qualité des données financières et de mieux évaluer les risques systémiques. L'identifiant international des acteurs des marchés financiers (LEI) peut également contribuer à identifier clairement les entreprises et à détecter les risques systémiques en utilisant les informations du registre des ayants droit économiques.
- En outre, le Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales a publié des recommandations sur la transparence des ayants droit économiques des personnes morales et évalue régulièrement leur mise en œuvre. Le respect des normes internationales est un objectif stratégique du Conseil fédéral, notamment en ce qui concerne les listes de l'UE des pays présentant un risque de blanchiment d'argent et d'évasion fiscale.

Principaux éléments

- L'introduction d'un registre fédéral des ayants droit économiques des personnes morales, géré par le DFJP et accessible aux autorités compétentes, aux intermédiaires financiers, aux conseillers et aux avocats, afin de satisfaire aux obligations de diligence en matière de blanchiment d'argent.
- La création d'une autorité de contrôle, rattachée au DFF, chargée de garantir la qualité du registre.
- Il y a pour les sociétés, de nouvelles obligations d'identifier, de vérifier et de mettre à jour leurs ayants droit économiques, et les actionnaires et les ayants droit économiques doivent coopérer à l'exécution de ces obligations.
- L'introduction d'obligations de ressortissants à la société et aux registres concernés pour les administrateurs, les directeurs, les associés et les actionnaires agissant à titre fiduciaire.

Destinataires de la loi

- Les personnes morales de droit suisse (SA, Sàrl, SICAV/SICAF, coopératives, fondations ainsi que les associations qui doivent s'inscrire au registre du commerce).
- Entités juridiques ayant leur siège à l'étranger, qui ont un lien étroit avec la Suisse et présentent des risques particuliers (par exemple, propriété immobilière, gestion effective en Suisse ou exploitation d'une succursale).

Recommandation GAFI de mars 2022

- Le Groupe d'action financière (GAFI) a adopté ses recommandations révisées sur la transparence des personnes morales et l'identification des bénéficiaires effectifs. La mise en œuvre de ces recommandations sera évaluée pour tous les pays membres dans le cadre du prochain cycle d'évaluation. La Suisse est membre du GAFI. En 2020 déjà, la Suisse avait fait l'objet de recommandations lui enjoignant d'améliorer encore la transparence des bénéficiaires effectifs des personnes morales. Selon toute vraisemblance, l'examen de la Suisse est prévu jusqu'en 2027.

Calendrier

Message du Conseil fédéral : 22 mai 2024

Entrée en vigueur dès 2026

Banques et maisons de titres: Directement concernés

Asset Management: Directement concernés

Gestionnaire de fortune et Trustees: Directement concernés

Risques opérationnels banques et Résilience opérationnelle

Révision de la circulaire FINMA
Créer la transparence nécessaire en ce qui concerne les risques opérationnels et la résilience opérationnelle

Principes de base et nouveautés

Remarques préliminaires

- La gestion des risques globaux et de leurs effets, tels que l'évolution des technologies de l'information et de la communication (TIC) et la numérisation, en particulier avec le stockage des données des clients dans des solutions en nuage, implique le respect d'exigences élevées en matière de sécurité des données pour les responsables du traitement (en référence à la nLPD et à l'OPDo révisées, entrées en vigueur le 1er septembre 2023).
- Les évolutions technologiques entraînent un déplacement du risque dans le secteur financier au détriment des banques et autres intermédiaires financiers.
- Le régulateur exige un examen préventif des normes de sécurité pour se protéger contre la perte ou l'altération de données (cyberrisques) afin de contrer de manière adéquate ces risques opérationnels («résilience opérationnelle»).

Concept de résilience opérationnelle et évaluation des risques

- La FINMA définit la résilience opérationnelle comme la capacité de l'établissement à pouvoir rétablir ses fonctions critiques en cas d'interruptions dans les limites de la tolérance aux interruptions, c.-à-d. la capacité de l'établissement à identifier les menaces et les défaillances éventuelles, à s'en protéger et à y réagir, à rétablir la marche ordinaire des affaires en cas d'interruptions et à en tirer des enseignements pour minimiser les conséquences sur l'exécution des fonctions critiques.
- Les perturbations opérationnelles et l'indisponibilité de services commerciaux clés sont susceptibles de causer un préjudice généralisé aux clients et à l'intégrité du marché, de menacer la viabilité des institutions et de provoquer l'instabilité du système financier.

Contenu essentiel

- Principe de proportionnalité: mise en oeuvre au cas par cas en fonction de la taille, de la complexité, de la structure et du profil de risque de l'établissement.
- Gestion globale des risques opérationnels dans le cadre de la gestion des risques à l'échelle de l'établissement : Le Conseil d'administration approuve les principes de base de la gestion des risques opérationnels pertinents et surveille leur application.

Il s'agit notamment de:

- La gestion des risques liés aux TIC (technologies de l'information et de la communication): Nécessite un haut niveau d'expertise de la part de tous les membres impliqués.
  - Les cyberrisques
  - Risques concernant les données critiques
  - Risques liés à la conception et à la mise en oeuvre du BCM (Business Continuity Management)
  - Risques liés aux activités transfrontalières

Champs d'action

Conseil d'administration (CA):

- Définition d'une stratégie TIC (orientation et développements technologiques) et surveillance de l'efficacité de la gestion des TIC.

Direction générale (DG):

- Mise en oeuvre de la stratégie TIC, gestion des risques liés aux TIC et garantie de ressources adéquates. Assurer la fiabilité, l'intégrité et la disponibilité des TIC utilisées.

Rapports internes et contenu cm 41 ss Circ.-FINMA 23/1:

- Prise en considération des facteurs externes tels que les événements de perte reconnus d'autres institutions, les changements de la situation de sécurité (par exemple en raison d'influences environnementales, de cyberattaques ou de terrorisme) ou les changements dans les exigences réglementaires; Vue d'ensemble de l'efficacité des contrôles clés et prise en compte des risques opérationnels nouvellement apparus.
- Résultats de l'application d'outils et de méthodes supplémentaires conformément au cm 33 de la Circ.-FINMA 23/1 «Risques et résilience opérationnels – banques», tels que la collecte et l'analyse systématiques des données de pertes internes et des événements externes pertinents.

Opérations ICT (exploitation et maintenance) cm 53 ss Circ.-FINMA 23/1:

- Maintenir un inventaire de tous les composants des TIC (matériel, logiciel et emplacement des données critiques); l'inventaire doit être disponible en temps utile et régulièrement revu et mis à jour. Mise en place des processus, procédures et contrôles pour garantir la confidentialité, l'intégrité et la disponibilité de l'environnement TIC (y compris la sauvegarde et la récupération).

Gestion des incidents («Incident Management») cm 58 ss Circ.-FINMA 23/1:

- Mise en place des procédures, processus et contrôles pour atténuer le risque d'incidents de sécurité. Définition des rôles et responsabilités pour le traitement des incidents et lien entre les incidents TIC et le BCM (Business Continuity Management) ainsi que le DRP (Disaster Recovery Plan).

Calendrier

Entrée en vigueur: 1er janvier 2024

- Délai de transition: En ce qui concerne la garantie de la résilience opérationnelle, il existe pour les destinataires un délai de transition de deux ans (cf. les références correspondantes dans la Circulaire 2023/01, ch. 113)
- Pour certaines exigences particulières (comme celles relatives à l'inventaire), une période d'entrée en vigueur s'applique. Délai de transition d'1 an à compter de l'entrée en vigueur

Banques et maisons de titres: Directement concernés

Asset Management: Indirectement ou partiellement concernés

Gestionnaire de fortune et Trustees: Pas concernés

Risques opérationnels banques et Résilience opérationnelle (2)

Principes de base et nouveautés

Gestion des cyberrisques cm 61 ss Circ.-FINMA 23/1

- Pour pouvoir faire face à la technologisation nécessaire, les cyberrisques doivent être intégrés de manière transparente dans l'inventaire des risques opérationnels. Rapport annuel sur les cyberrisques à l'intention de la direction générale (efficacité des contrôles, cyberévénements); exigences minimales à prendre en compte dans le cadre du système de contrôle interne (SCI): i) Identification des cyberrisques sur la base de l'inventaire informatique et du portefeuille de processus opérationnels; ii) Mise en oeuvre de procédures et de contrôles de surveillance des systèmes pour détecter et répondre aux cyberattaques (y compris la déclaration obligatoire des cyberattaques à la FINMA et l'analyse de suivi appropriée).
- Planification des procédures de reprise des activités en cas de cyberattaques. Mise en place de programmes obligatoires de sensibilisation aux cyberrisques pour les employés et mise en place d'évaluations périodiques de la vulnérabilité et de tests d'intrusion.

Gestion du risque lié aux données critiques cm 71 ss Circ.-FINMA 23/1

- La circulaire révisée inclut dans la gestion des risques les dimensions de confidentialité, d'intégrité et de disponibilité des données dites critiques. Ceci est conforme au BCBS (Comité de Bâle sur le contrôle bancaire).
- Les données critiques sont des données qui nécessitent une protection particulière. Il appartient à la banque de classer les données en fonction du risque.
- Mise en place et documentation de la gestion des données critiques, conformément à une stratégie de données définie.
- Définition des processus, contrôles, rôles et responsabilités liés aux données critiques.
  - Respect des exigences en matière de confidentialité, d'intégrité et de disponibilité des données critiques
  - Protection des données critiques stockées en dehors de la Suisse
  - Signalement sans délai des incidents à la FINMA
  - Due diligence pour la sélection des prestataires de services qui ont accès aux données critiques (définition des critères et mise en place d'examens périodiques).

Business Continuity Management (BCM) cm 83 ss Circ.-FINMA 23/1

- Les exigences BCM contraignantes jusqu'à présent ont été reprises avec des affinements. Les exigences BCM doivent être adaptées en cas de délocalisations significatives. Avant l'entrée en vigueur de la nouvelle circulaire le 1er janvier 2024, le CA doit approuver les «objectifs de continuité» (également appelés «tolérances aux interruptions») ainsi que les «fonctions critiques»*.

* Fonctions critiques: Processus, services et ressources nécessaires à leur fourniture, dont l'interruption mettrait en péril la pérennité de l'établissement ou son rôle sur le marché financier.

Résilience opérationnelle -cm 101 ss Circ.-FINMA 23/1 «Risques et résilience opérationnels – banques»:

- La FINMA définit la résilience opérationnelle comme la capacité de l'établissement à pouvoir rétablir ses fonctions critiques en cas d'interruptions dans les limites de la tolérance aux interruptions, c.-à-d. la capacité de l'établissement à identifier les menaces et les défaillances éventuelles, à s'en protéger et à y réagir, à rétablir la marche ordinaire des affaires en cas d'interruptions et à en tirer des enseignements pour minimiser les conséquences sur l'exécution des fonctions critiques. Les perturbations opérationnelles et l'indisponibilité de services commerciaux clés sont susceptibles de causer un préjudice généralisé aux clients et à l'intégrité du marché, de menacer la viabilité des institutions et de provoquer l'instabilité du système financier.
- Les éléments suivants permettent de soutenir la résilience opérationnelle:
  - Focalisation avec une vue top-down (top=BoD) sur les opérations les plus stratégiques (appelées «fonctions critiques» dans la circulaire)
  - Identification des fonctions critiques et de leurs tolérances aux risques, qui doivent être approuvées (annuellement) par le CA.

Calendrier

Entrée en vigueur dès 2024

Banques et maisons de titres: Directement concernés

Asset Management: Indirectement ou partiellement concernés

Gestionnaire de fortune et Trustees: Pas concernés

CONTACTEZ-NOUS

N'hésitez pas à prendre contact avec nous pour plus d'informations concernant les thèmes abordés ou concernant nos prestations de services Regulatory & Compliance:

TAULANT AVDIJA
Responsable Regulatory & Compliance Suisse
taulant.avdija@bdo.ch

PATRICK CATTIN
Responsable Audit Financial Services Suisse romande
patrick.cattin@bdo.ch

BDO SA
Rte de Meyrin 123
Case postale 150
1215 Genève 15
Tél. +41 22 322 24 24

BDO SA

BDO SA est l'une des plus importantes sociétés suisses d'audit, de services fiduciaires et de conseil. Ses compétences clés englobent les prestations d'audit, les services fiduciaires, le conseil fiscal et juridique ainsi que le conseil d'entreprises. Avec ses 36 succursales, l'entreprise dispose du réseau le plus dense de la branche. La proximité et la qualité des compétences sont des valeurs essentielles pour ses 1'600 collaborateurs. De cela découle des relations durables avec les clients. La première succursale entièrement digitale offre aux PME la possibilité de traiter des opérations simples et standardisées de manière automatisée. BDO SA révise et conseille des entreprises actives dans les secteurs de l'industrie et des services, notamment des PME, des sociétés cotées en bourse, des administrations publiques et des organisations à but non lucratif.

Le réseau international BDO, qui couvre plus de 160 pays, est à disposition des entreprises orientées vers l'international. BDO SA a son siège principal à Zurich et est le membre suisse, juridiquement indépendant, du réseau international BDO, dont le siège est à Bruxelles (Belgique).

www.bdo.ch