BDO

Sharing mindsets – shaping the future

Regulatory & Compliance Update

Proposed or newly enacted regulations and current regulatory projects in banking and asset management

March 2024

Contact:

Susanne De Zordi
Head of Financial Services
Partner

Dr. Detlev Michael Basse
Head of Regulatory & Compliance, German-speaking Switzerland
Director

Taulant Avdija
Head of Regulatory & Compliance Switzerland
Partner

Patrick Cattin
Head of Audit, Western Switzerland
Partner

Contents

DImportant note:

In the following we provide an overview of important Swiss financial market law regulations that have recently entered into force. The overview also covers international financial market law and international regulations, especially from the EU, insofar as the provision of products and services from Switzerland to other countries results in an obligation to comply with the respective foreign legislation (e.g. investor protection). Also included in this overview are upcom- ing regulatory projects, enabling those affected to plan any imple- mentation projects for the legal or regulatory requirements at an early stage.

These regulations primarily apply to banks, securities firms, asset management institutions (fund management companies, managers of collective assets, SICAVs, SICAFs, limited partnerships for col- lective investment, other collective investment schemes, custodian banks of collective investment schemes, representatives), portfolio managers and trustees.

Not all entities are affected to the same extent by legal and regula- tory changes due to their business model (market services) and their geographical coverage (national or international). Insurers are not included in the overview.

The overview contains a selection of regulations/projects which, in our view, are of particular importance due to their scope and im- pact, including with regard to new processes and necessary controls (ICS). There is no guarantee that the information presented in the following overview is complete and accurate. BDO does not assume any liability for it. BDO accepts no liability whatsoever for any loss or damage arising on the basis of this overview. The overview does not release the addressees from their obligation to familiarise them- selves in detail with the original legal basis or legal and regulatory changes. BDO reserves the right to simplify the presentation in the overview.

▶ Part 1

Proposed or enacted changes

Contents

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Automatic Exchange of Information (AEOI) Multilateral Competent Authority Agreement (MCAA), including Common Reporting Standard (CRS) as international legal basis (OECD) AEOI Act, AEOI Ordinance and SFTA Guidelines on the Standard for Automatic Exchange of Financial Account Information in Tax Matters as a CRB (8 January 2021)	• Switzerland implements AEOI in principle on the basis of the Multilateral Competent Authority Agreement (MCAA) on the automatic exchange of financial account information. AEOI has been agreed with the EU, Hong Kong and Singapore on the basis of bilateral treaties. • The list of activated bilateral exchange relations of all states and territories can be viewed on the OECD website. This list sets out Switzerland's AEOI partner states. It is updated regularly and is more authoritative than the OECD lists. • Partner states from 1 January 2024: - Thailand (reciprocal jurisdiction) - Kenia (reciprocal jurisdiction) Note: If a state declares itself as a "permanent non-reciprocal jurisdiction", it provides account information to the partner states on a long-term basis but the state or territory does not receive such data. • Automatic reporting concerns four categories of financial institutions ("reporting institutions"): i) depository institutions, ii) custodial institutions, iii) investment entities and iv) specified insurance companies. • Reporting obligations for Swiss FIs (section according to the guidelines): - Registration with the SFTA (see section 10.1), - Fulfilment of the due diligence requirements for the identification of reporting accounts (cf. section 6), - Information duties vis-à-vis clients (cf. section 8), and - Reporting to the SFTA of the information to be exchanged in relation to reportable accounts (cf. section 7). **Transmission deadlines** • The reporting Swiss FIs transmit the information electronically to the SFTA annually by 30 June at the latest following the end of the calendar year to which the information relates. **Changes to the AEOI model** • International automatic exchange of information in tax matters is to include crypto assets in future (SIF press release dated 10 November 2023). In a joint declaration, around 50 countries, including Switzerland, have today committed to the expanded international automatic exchange of information in tax matters (AEOI). The expansion (Crypto-Asset Reporting Framework, CARF) concerns crypto assets and is to apply from 1 January 2026. CARF regulates the handling of crypto assets and their providers. **Objective** • The CARF is intended to close gaps in the tax transparency mechanism and ensure that providers of crypto assets are treated in the same way as the traditional financial sector. Implementation of the CARF will enhance Switzerland's progressive crypto market regulation and contribute to the credibility and reputation of the Swiss financial centre. **Consultation** • The Federal Department of Finance (FDF) will prepare a consultation draft for implementation of the expanded AEOI by the end of June 2024. Switzerland also intends to implement the CARF.	• By 30 June 2023: Observe reporting obligations with regard to all partner states (including for the first time states with which Switzerland will apply AEOI from January 2023). • Perform an initial review of the data basis of the financial assets/ accounts concerned with regard to AEOI-relevant changes (e.g. third country departure), referring to current partner states (see SIF list). • Look at control framework with verification of changes and reconciliation with AEOI parameters; see also AMLA (AML) duty to periodically review client documentation applying a risk-based approach since 1 January 2023	**New AEOI partner states: 1 January 2024** (see background and changes) Expansion of the AEOI model with crypto assets from 1 January 2026 Preparation of FDF consultation draft by 30 June 2024

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Not affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Investor protection/organisational measures for financial service providers Financial Services Act (FinSA) Financial Services Ordinance (FinSO)	• The Financial Services Act (FinSA) was created to improve investor protection by tightening due diligence and organisational obligations for financial service providers (FS providers) and to balance the knowledge gap between investors inexperienced in financial transactions and financial service providers. FinSA also achieves alignment with the European regulations (MiFID II/MiFIR, etc.) • Duty to inform clients prior to the conclusion of the contract or execution of the transaction, providing details of the costs and fees as well as special conditions charged by the bank for its services. This mandatory information and any adjustments must be communicated in good time. • Customer segmentation: Subdividing all investor clients into private, professional or institutional clients. For this, there are possibilities to - opt in or out of the individual customer categories; also includes notification that professional and institutional clients have the option to opt-in (no influence of the FS provider on the client's decision; no prohibitive effect) - Opting out requires that the client can make an independent decision and has also been informed about the opportunities and risks of losing stricter investor protection and the associated loss of rights. • Art. 6a CISO requires the FS provider (FI) to inform investors (cf. Art. 10 para. 3ter CISA) that they are deemed qualified investors; explain the risks that this entails; inform them that they have the option of not wishing to be deemed qualified investors. • New Code of Conduct: Suitability assessment of financial products and services, depending on the client segment and type of service; investment advice provided in consideration of the client portfolio (portfolio context; not transaction-related) or implementation of an AM mandate requires a suitability assessment for private clients: financial situation with income and assets (see Art. 5 FinSO, such as precious metals and life insurance policies with a surrender value); incl. current and future commitments such as intended loan; in the case of agency relationships, the FS provider takes into account the experience of the person representing the client (governed in the power of attorney); exceptions to the verification requirement for execution only (irrespective of the complexity of the financial instrument) and for professional clients (incl. high-net-worth retail clients pursuant to Art. 5 FinSA). • The FS provider may rely on the information provided by the client unless there are indications that it does not correspond to the facts (cf. Art. 17 para. 3 FinSO); no plausibility check required by the FS provider. • FS provider asks about the investment objectives with details, in particular of the time horizon, purpose of the investment; of the client's risk capacity and willingness; and of any investment restrictions (security restrictions). • General duty to prepare a prospectus for public offering of securities. • Before offering a financial instrument to retail clients, a key information document (KID) must be prepared (e.g. electronic publication on the FS provider's website), which contains essential information for making investment decisions and making comparisons between different financial instruments; a KID is deemed to be available if it can be found with a reasonable amount of effort; when executing and transmitting client orders, private clients may generally consent to the KID only being made available after the transaction has been concluded; consent must be given separately to agreement to the general terms and conditions (GTC) in writing or in another form that allows proof by text (cf. Art. 11 FinSO); it is not permissible to agree on a waiver of subsequent provision. • Organisational measures (Art. 21 et seq. FinSA/23 et seq. FinSO): - Appropriate precautions to prevent conflicts of interest (risk-based). - Issue of internal directives (with reference to the recognition of conflicts of interest and identification of measures to prevent conflicts as well as the duty to regularly review them).	• Implement customer segmentation on the basis of the customer's independent decision/legally sufficient information on the implications of opting out. • Introduce transparent forms for opting-out and opting-in. • Implement appropriateness and suitability check in forms and systems. • Implement information duties by means of leaflets and/or website. • Implement documentation and accountability reports. • Implement organisational duties. • Implement duties regarding prospectus and KID. • Duty to affiliate to an ombudsman (except for institutional and per se professional clients only). • For client advisors: Duty to take part in education and training (ensuring specialist qualifications).	**Entry into force: 1 January 2020**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Financial institutions/external portfolio managersr Financial Institutions Act (FinIA) Financial Institutions Ordinance (FinIO) Ordinance on Supervisory Organisations in Financial Market Supervision (SOO) Draft FINMA Financial Institutions Ordinance (FinIO-FINMA) Late applications, FinIA	• FinIO clarifies the licence requirements and obligations for financial institutions as well as supervision of them. • The SOO governs the licensing requirements and the activities for the newly introduced supervisory organisations • In particular, the FinIO-FINMA sets out the distinction between ordinary portfolio managers and managers of collective assets and the requirements for professional liability insurance as well as for risk management and risk control. As part of this process, various FINMA circulars were also amended and/or repealed and the threshold value requiring customer identity checks in foreign exchange transactions in cryptocurrencies was lowered from CHF 5,000 to CHF 1,000. • The requirements for securities firms regarding capital and liquidity are now different depending on whether the firm operates for its own account or not (cf. Art. 41 FinIA). • The SOs carry out a preliminary review of the applications in accordance with FINMA's specifications. However, it is not their task to ensure that institutions meet the applicable deadlines (guidance, p. 6). • Filing the application with FINMA incl. confirmation of affiliation with a SO by 31 December 2022 = business activity of the portfolio manager (PM) can be continued until the licensing decision has been made. (cf. guidance, section 3.1). **FINMA Guidance 01/2024** • In its supervisory communication of 2 February 2024, FINMA states that as at 31 December 2023, it had approved 1,149 (70%) of the licence applications received by 31 December 2022 and that 63 institutions (4%) had withdrawn their application. The 487 remaining applications (26%) are more complex and require a longer processing time. Institutions that remain affiliated with a self-regulatory organisation and have submitted their licence application with proof of affiliation to a supervisory organisation (SO) to FINMA before the end of the transition period can continue their business activities.	• Institutions already authorised by FINMA: Compliance with FinIA requirements within one year • Investigations in 2023: Institutions that were already operating before FinIA entered into force and do not submit an application to FINMA by the end of 2022 may no longer conduct their business (on a professional basis) as of 1 January 2023. • Institutions that intentionally or negligently act without authorisation must reckon with the previously mentioned consequences under supervisory law and criminal law (cf. guidance 03/2023, section 3). • FINMA will report these cases to the prosecution authorities under its criminal complaint procedure and will initiate investigations (guidance 03/2023, section 3.3	**Entered into force:** • FinIO-FINMA: 1 January 2021

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Indirectly or partially affected	Directly affected	Directly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Company law (CO) Art. 620 et seq. (revision of the law)	On 1 January 2023, the remaining provisions of the revised company law entered into force. The following areas are affected by the changes: **• Capital structure** - Share capital, which must still amount to at least CHF 100,000, may be held in a permissible foreign currency such as euros, US dollars or pounds sterling, provided that this is the company's main currency (for business operations). A change of cur-rency is possible at the beginning of each financial year. - The nominal value of shares may be less than CHF 0.01, but must be greater than zero - A capital band is introduced allowing 50% more or 50% less than the registered share capital. Within the capital band, the BoD may reduce or increase the share capital within a maximum of five years. - Removal of the provisions on the intended acquisition of assets at the time of incorporation or capital increase. - Permissibility of distributing interim dividends from current operations. - Permissibility of repayment of the statutory capital reserve (premium and other contributions exceeding the nominal value) to the shareholders under certain conditions. **• Shareholder rights and duties of the board of directors (BoD)** - Shareholders of companies whose shares are not listed on a stock exchange and who hold at least 10% of the share capital or voting rights may ask the board of directors questions at any time (not only at the AGM). The BoD must provide the information within four months. - Shareholders of private SMEs holding at least 5% of the share capital or voting rights have the right to inspect the accounts and correspondence without the need for authorisation by the AGM, provided that this is necessary in order to exercise the shareholders' rights, subject to the legitimate interests of the company. - Reduction to 5% of the threshold of minority shareholders in private SMEs for the inclusion of items on the agenda of the AGM and for the convocation of an extraor-dinary AGM. - The BoD must continuously monitor the liquidity of the company. If there is a justified concern of imminent insolvency, the BoD is obliged to take appropriate measures to ensure liquidity and, if necessary, to initiate additional restructuring measures. The board of directors is no longer required to file the balance sheet with the bankruptcy court in the event of over-indebtedness if there is a reasonable pros-pect that the over-indebtedness can be remedied within a reasonable period of time (no later than 90 days after the audited interim financial statements are available). Creditors' claims must not be additionally jeopardised. - The previous provision on the appointment of a secretary to the board of directors has been deleted. The minutes may be signed directly by the minute-taker instead of the secretary. **• Place and manner of holding the annual general meeting (AGM)** - Convening a general meeting: may be requested by one or more shareholders who together represent at least 10% of the share capital; new: extension of this threshold to the number of votes (however, the amount remains the same for non-listed com-panies). For listed companies a threshold of 5% is now sufficient (cf. Art. 699 CO). - Right to request and place items on the agenda: Shareholders of listed companies representing 0.5% of the share capital or votes may request that an item be placed on the agenda; for all other companies, a threshold of 5% of the share capital or votes now applies (instead of a nominal value of CHF 1 million as before); (cf. Art. 699b CO). - Use of digital technologies when holding AGMs: virtual AGMs (e.g. video confer-ences) may be held (including AGMs held at different venues or abroad, provided that this does not unduly impede the exercising of shareholders' rights). Universal meetings may now be held electronically or in writing. **• Further changes** - Shareholder claims: The AGM can now resolve that the company must file a claim for restitution or a liability claim against a negligent body such as the board of directors or the auditors. The relative statute of limitations for liability claims is now only three years. - Special investigation: Reduction of the threshold for the initiation of a special inves-tigation (previously special audit) by shareholders of public companies to at least 5% of the share capital or votes instead of 10% under the old law (cf. Art. 697d CO). - Action for dissolution: a shareholder may also, individually or jointly with several shareholders representing at least 10% of the share capital or votes, demand dissolu-tion for important reasons.	• Amend the Articles of Asso-ciation and Organisational Regulations • Provisions that contradict the new company law shall remain in force until no later than 1 January 2025 at the latest and must be amended by then. • Provisions of the articles of association in accordance with the new company law may al-ready have been included in the articles of association prior to the entry into force of the new law. The articles of association must state that these new pro-visions will not come into force until 1 January 2023. • Recommendation to private SMEs to review the existing articles of association and regulations and decide when they should be adapted. • The holding of virtual AGMs as well as AGMs abroad requires a provision in the company's articles of association. • Gender quota of 30% (board of directors) and 20% (manage-ment board) with "comply or explain" approach for large list-ed companies, i.e. companies exceeding two of the thresholds of Art. 727 para. 1 no. 2 CO (CHF 20 million balance sheet total, CHF 40 million sales rev-enue, 250 full-time positions) in two consecutive financial years; if the minimum thresholds of Art. 734f CO are not met, the BoD must submit a report in accordance with Art. 716a para. 1 no. 8 CO (remuneration report) stating the reasons and the measures taken to promote the less strongly represented gender. • Transitional provisions with regard to the BoD no later than five years and with regard to the executive committee no later than ten years after the new law enters into force, i.e. as of 1 January 2026 and 1 January 2031, respectively.	**Entered into force:** 1 January 2023; articles of association to be amended by 1 January 2025 at the latest

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected/indirectly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Data protection/ data security	**Objectives of modern data protection (nFADP and EU GDPR)** • Protection of natural persons in the processing of personal data (fundamental right). • Consistent and high level of data protection for natural persons due to rapid technological developments and through globalisation ("Big Data" as a challenge for data protection and the right to privacy; e.g. profiling). • The protection of natural persons should be technology-neutral and not depend on the techniques used (data protection by design and by default). **Background** • The totally revised Data Protection Act (FADP) and the implementing provisions in the new Data Protection Ordinance (DPO) and the new Ordinance on Data Protection Certification (DPCO) entered into force on 1 September 2023. • The totally revised FADP and the corresponding provisions in the ordinances will ensure better protection of personal data for natural persons (purpose) in the future. In particular, data protection is adapted to technological developments, self-determination over personal data is strengthened and transparency in the procurement of personal data is increased. • The Federal Council has amended the draft DPO in several points: - Revision of the chapter on the duties of the responsible persons - Exemption of private individuals from certain information obligations when disclosing personal data. - Simplification of the modalities for the right of access; in particular, the documentation requirement has been deleted. - Adjustment in some respects the area of data security (reason: critical feedback from the consultation process). - Definition of a period of at least one year for the storage of protocols on data processing. - Insertion of a new provision that harmonises the protective objectives in the area of data security with the new Information Security Act of 18 December 2020. **Principle** • Presumption of lawfulness of data processing if required for the performance or planned conclusion of a contract and the purpose of the processing is for a specific purpose that is apparent to the data subject; for marketing purposes, additional [electronic] consent is required from the data owner. **Application of EU General Data Protection Regulation (GDPR)** • The marketplace principle governs and extends the territorial scope of application of European data protection law by data processors outside the EU when processing personal data, provided that the respective offer is directed at the European market ("marketplace"). • For responsible companies (controllers), this means that the GDPR is fundamentally applicable to target markets in the EU. As a result, they are also subject to the substantial catalogue of fines under the GDPR (prescribed for all EU member states) in the event of a violation of provisions. The mere making available of a website, an e-mail address or other account data or the use of a language that is commonly used in the third country in which the controller is established is not sufficient for the application of the marketplace principle; in contrast, any form of web tracking (observation, collection, evaluation of the surfing behaviour of data subjects on the Internet), known as "profiling" (cf. Art. 5 lit. f nFADP or Art. 4 No. 4 GDPR). **Legal comparison** • Compatibility of Swiss law with EU law, in particular with the General Data Protection Regulation (GDPR). • The nFADP is intended to ensure that the free movement of data with the European Union can be maintained so that Swiss companies do not lose competitiveness (cf. www.kmu.admin.ch).	• Review existing directives and work instructions on the topic of data protection and data security. • Revise/amend contracts relating to the outsourcing of processing activities to processors by the controller with a view to the protection of personal data, including data security (especially cloud solutions); ensure an equivalent level of data protection (Swiss or EU standard); cf. Art. 9 FADP and Art. 7 DPO. • Review the consent requirements of the data subject according to the categories of personal data processed; in particular, explicit consent for particularly sensitive personal data pursuant to Art. 5 lit. c in conjunction with Art. 6 para. 7 6 para. 7 nFADP. • Create or update data protection directory (Records of processing activities/ROPA) pursuant to Art. 12 nFADP or Art. 30 GDPR in accordance with the statutory minimum requirements; exemption from the obligation to maintain a ROPA: SMEs and other organisations under private law that employ fewer than 250 employees on 1 January of a year, as well as natural persons; duty to maintain a ROPA if: Processing particularly sensitive personal data on a large scale or carrying out high-risk profiling. • Ensure right of access free of charge for data subject within 30 days of request in accordance with Art. 25 nFADP and Art. 16 et seq. nDPO. • Appoint a data protection officer in accordance with Art. 10 FADP (optional provision for private data controllers); tasks and requirements in accordance with Art. 26 nDPO. • Recommendation: Appoint a data protection officer for companies with 250 or more employees (direct contact person for the FDPIC; central monitoring for data protection ensured). • Data protection impact assessment (DPIA) for data processing with a high risk to the privacy or fundamental rights of the data subject (e.g. project mandate and DPIA as a component). • Training/education of employees on data protection and data security. • Develop control framework (ICS). • Conduct IT penetration tests to close security gaps and run awareness trainings.	**Entered into force:** 1 September 2023 nFADP, nDPO and Ordinance on Data Protection Certification (DPCO)

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Anti-money laundering **Revision of AMLA and AMLO (Federal Council)**	**Overview** • With the revised AMLA and the Federal Council's AMLO, Switzerland is improving its defensive measures to combat money laundering and terrorist financing (implementation of the recommendations of the FATF Country Report (of the Financial Action Task Force/FATF). • The measures for financial intermediaries include: - Stricter requirements for establishing beneficial ownership through new verification obligation. - Financial intermediary has a duty to periodically update client data in accordance with a risk-based approach (active conduct). - Legal basis for reporting suspicion of money laundering (cf. Art. 9 para. 1quater AMLA, in force since 1 January 2023): reasonable suspicion if the financial intermediary has a concrete indication or several indications that paragraph 1 letter a could be met for the assets involved in the business relationship and this suspicion cannot be dispelled on the basis of additional clarifications pursuant to Art. 6 AMLA. - Better transparency of associations with increased risk in the area of terrorism financing; i.e. associations that mainly collect or distribute assets abroad, directly or indirectly, intended for charitable, religious, cultural, educational or social purposes are required to be entered in the commercial register; all associations subject to registration must keep a register of members and be able to be represented by a person domiciled in Switzerland (cf. Art. 61 para. 2 no. 3 nCC and Art. 61a nCC). - Increased supervision and controls in the area of precious metals. **Notes for practice:** 1. Obligations in the event of suspicion of money laundering are no longer laid down in ordinances of the supervisory authorities, but are regulated by the Federal Council. 2. Simply producing copies of the beneficial owner's identification documents does not meet the requirements for verification; check plausibility with other information (e.g. KYC profile) and file notes (traceability). 3. The duty to periodically update client information is not a new one as in practice the financial intermediaries already have to periodically check the information of their clients as part of the risk categorisation. The duty to periodically check that client data is up to date applies to all business relationships regardless of the risk. However, with regard to the periodicity, scope and nature of the review and updating of client data, a risk-based approach was chosen. The risk-based approach is the outcome of differentiated and proportional regulation. It enables financial intermediaries to adopt individualised risk management tailored to their business model and client population. 4. An exemption from the registration requirement in the commercial register is provided for smaller associations. In addition, under certain conditions, their entry in the commercial register can be waived for the protection of travelling board members. →See below for FINMA's guidance on the requirements of the money laundering risk analysis pursuant to Art. 25 para. 2 AMLO-FINMA.	• Add action fields to the AML/CTF or AML/ KYC directive to verify the BO or the control holder in accordance with the declaration on Form A or K CDB 20 or other applicable forms (comparison with KYC data). • Add content to the AML/CTF or AML/KYC directive regarding criteria for the risk-based, periodic review of the up-to-dateness of client information and the (control) processes (e.g. high-risk clients with annual review; clients with medium risks every 2-3 years; local clients with low risks every 4-5 years). • When onboarding new clients with the legal form "association" (CC 60), i.e. written articles of association, review of the purpose of the association with regard to requirements according to Art. 61 CC; review of existing "association" clients in connection with periodic review of documentation. • Note: Association according to Art. 61 CC falls under higher risk category (risk categorisation according to AMLO-FINMA).	**Entry into force of revAMLA and AMLO:** 1 January 2023; the Federal Council has already put the first part of the revised AMLA into force for trade assayers for precious metals as of 1 January 2022 **Entry into force of Art. 61 para. 2 no. 3 and Art. 61a CC: 1 January 2023**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
FATF – recommendations to combat money-laundering Updated country list (high risk jurisdictions) Jurisdictions with strategic AML/CFT deficiencies (Amendment of EU Regulation and Adjustment for Liechtenstein's Due Diligence ACT ("SPG")	**Background** • The Financial Action Task Force (FATF) is an international association that serves to develop and promote measures to combat money laundering and to fight terrorism and proliferation financing. Switzerland is a member of the FATF. • As of October 2023, the FATF had reviewed 129 countries and jurisdictions and publicly identified 102 of them. Of these, 76 have since implemented the necessary reforms to address their weaknesses in combating money laundering and terrorist financing and have been removed from the process (see www.fatf-gafi.org/en/countries/black-and-grey-lists.html). **Virtual assets (crypto assets)** • Virtual assets have many potential benefits and dangers. They have the scope to make payments easier, faster and cheaper, and provide alternative methods for those without access to regular financial products. However, they are largely unregulated, and also have the potential to become worthless and are vulnerable to cyberattacks and scams. • Without proper regulation, virtual assets also risk becoming a safe haven for the financial transactions of criminals and terrorists. The FATF has been closely monitoring developments in the cryptosphere and has issued global, binding standards to prevent the misuse of virtual assets for money laundering and terrorist financing (see www.fatf-gafi.org/en/topics/virtual-assets.html). **Action required by financial institutions with crypto assets** • Countries must prioritise full and effective implementation of the FATF standards for virtual assets. At the same time, providers of virtual assets must implement the same preventive measures as financial institutions, including customer due diligence, record keeping and reporting of suspicious transactionsn. • FINMA has issued the following guidance relevant to supervisory law: - Travel Rule for Virtual Asset Service Providers (VASP) 08/2019 - „Staking" guidance 08/2023 of 20 December 2023 (with reference to variants in practice and principles of custody) **"High-risk jurisdictions" (FATF)** • High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing risks emanating from the country. This list is often externally referred to as the "blacklist". (3 March 2024: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html) • FATF high-risk jurisdictions: North Korea, Iran and Myanmar. **FATF jurisdictions under increased monitoring (FATF)** • Jurisdictions under increased monitoring are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the "grey list".	• Review and potentially revise business relationships with elevated risks pursuant to Art. 13 paras. 2 and 3 lit. d AMLO-FINMA with direct reference to the FATF list of jurisdictions considered "high risk" or non-cooperative, (nationality of the contracting party or beneficial owner of assets or type and location of business activity of the contracting party or beneficial owner of assets or country of origin or destination of frequent payments, namely payments from or to a country considered "high risk" or non-cooperative by the FATF). • Categorisation is decisive for risk classification and periodic updating of client documentation (annually for high-risk clients); incl. AML transaction monitoring.	**Publication: October 2023**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
	FATF jurisdictions on the "grey list"(as of 23 February 2024) • Barbados, Bulgaria, Burkina Faso, Cameroon, Croatia, Democratic Republic of Congo, Gibraltar, Haiti, Jamaica, Mali, Mozambique, Nigeria, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Turkey, Uganda, United Arab Emirates (UAE), Vietnam und Yemen **Jurisdictions with strategic deficiencies** • According to the Commission's draft Delegated Regulation (EU) 2023/... of 18 August 2023, Delegated Regulation (EU) 2016/1675 is to be amended. This is directly relevant for the obligations pursuant to Art. 11a of the Liechtenstein Due Diligence Act ("SPG") concerning states with strategic deficiencies. A change in the classification of risk countries by foreign states also increases the risk classification of clients or beneficial owners (BO) domiciled/ registered in these countries for Swiss banks and other financial intermediar- ies within the scope of the FINMA Guidance on AMLO-FINMA requirements for the money laundering risk analysis pursuant to Art. 25 para. 2 AMLO- FINMA.		

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
SECO sanctions, EU and OFAC/FC sanctions against Russia	**Background** • On 28 February 2022, the Federal Council (FC) decided to adopt the EU sanctions against Russia. The Swiss ordinance was therefore subject to a total revision on 4 March 2022. • In particular, Art. 20 and 21 should be highlighted for banks: - Prohibition on accepting deposits in excess of CHF 100,000 from Russian citizens or natural/legal persons in Russia (Art. 20; per client; with exemption provisions for Swiss citizens, citizens of a member state of the EU and natural persons who hold a temporary or permanent residence permit from Switzerland or a member state of the EU). - Duty to report to SECO any existing deposits of over CHF 100,000 of Russian citizens or natural/legal persons in Russia by 3 June 2022 (Art. 21). On 16 March 2022, SECO published an interpretation of these ordinance articles. **Updated sanction notice of 28 February 2023 (FC)** • On 28 February 2022, the Federal Council decided to adopt the European Union's (EU) sanctions against Russia and thus strengthen their effect. The existing Ordinance (SR 946.231.176.72) was therefore subjected to a total revision on 4 March 2022. • The measures include, but are not limited to, prohibitions on dual-use goods, especially military goods and goods for military and technological enhancement or for the development of the defence and security sector, and prohibitions on the issuance and trading of transferable securities and money market instruments. • Further changes are published on an ongoing basis and can be found at the following link: https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos.html	• Ensure that no deposits exceeding CHF 100,000 are accepted from Russian citizens and persons/companies resident in Russia (per client; taking into account the exemption provisions). • Check the client base for Russian citizens and persons/companies resident in Russia. • Report deposits of Russian citizens and persons/companies resident in Russia to SECO by 3 June 2022. • In accordance with the provisions of the ordinance, FIs are requested to implement the prohibitions, to freeze the assets of the sanctioned persons and to report the affected business relationships to SECO. • Reporting to SECO does not release an FI from the obligation to carry out additional investigations pursuant to Art. 6 AMLA in the event of suspicious circumstances and, if it is unable to dispel these suspicions, to immediately file a report with MROS pursuant to Art. 9 AMLA.	**Entry into force: ongoing monitoring and updating of sanctions lists**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Indirectly or partially affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
Money laundering risk analysis FINMA Guidance 05/2023 Money laundering risk analysis pursuant to Art. 25 para. 2 AMLO-FINMA	**Overview of the FINMA Guidance and relevant points for practical implementation** • Pursuant to Art. 25 para. 2 AMLO-FINMA, banks are obliged to prepare a money laundering risk analysis appropriate to the client relationship and the respective area of activity. Based on this, they must also determine the relevance for their own business activities (cf. Art. 13 para. 2 AMLO-FINMA) and prepare a corresponding risk analysis (cf. Art. 6 para. 1 lit. a AMLO-FINMA). In connection with this, the bank must take into account the close interdependency with its own risk policy on the business strategy and review this regularly. Detailed information on the duty to capture, limit and monitor banking risks can be found in FINMA Circular 2017/1 "Corporate Governance – Banks". **Content** • More stringent requirements for the risk analyses of banks. • Requirement to adequately define the money laundering risk tolerance, including set limits. • Strengthening of structural elements (e.g. client segments, domicile, type of product, geographical reach, etc.) as a basic prerequisite for an effective risk analysis. **Money laundering risk tolerance** The basic features of risk monitoring and limitation as well as corresponding responsibilities and processes must be governed by suitable regulations, policies or internal guidelines (cf. Art. 19 AMLO-FINMA). • In particular, the following points must be reviewed and, if necessary, amended: - The definition of risk tolerance must include the deliberate exclusion of certain countries, client segments, services and/or products in order to be sufficiently adequate. - Processes for exceptions to policy (ETP) from the defined risk tolerance must be covered in internal guidelines, approved by the executive board and monitored by the highest governing body. - Key indicators for monitoring risk tolerance must be defined with sufficient precision and submitted to the executive board and the board of directors for monitoring purposes. **Money laundering risk analysis** The risk analysis includes all money laundering risks to which the financial intermediary is exposed as well as those which it identifies, captures, analyses and measures based on its area of activity or positioning. Based on these findings, the financial intermediary defines its measures for managing, controlling, reporting and monitoring the risks (see explanatory report on the partial revision of the AMLO-FINMA of 11 February 2015). • In particular, the following parameters should be taken into account to determine the overall risk: - Client's place of incorporation or domicile - Client segment - Products and services offered - Geographical presence of the institution - Further categories are to be determined individually depending on the business model of the respective bank and implemented in the risk analysis. • The following points need to be reviewed and adjusted if necessary: - The money laundering risk must be shown individually and comprehensibly for each individual risk category with regard to its inherent risk, control risk and the resulting net risk. - Measures with a risk-mitigating impact (control risk) on inherent risks must be described in sufficient detail including key figures and findings regarding effectiveness. - Assessment and comprehensible justification of the relevance of individual criteria in the risk analysis. - Definition of key figures (global and local) with reference to the respective risk exposures in the bank's client population as well as taking corresponding measures (e.g. expansion of compliance, adjustment of risk policy, etc.). - The defined risks are to be reviewed periodically in a consolidated risk analysis and amended where necessary.	**Potential need for action** In order to meet FINMA's requirements, particular attention should be paid to the following points in practical implementation and, if necessary, appropriate measures should be taken: • Correct client segmentation/account allocation • Correct performance of the suitability and appropriateness test (client profile, risk profile and investment strategy) • Compliance with information and documentation duties • Compliance with the provisions on best execution of client transactions • Compliance with the regulations on compensation to third parties • Handling of conflicts of interest	**Publication:** **24.08.2023**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Indirectly or partially affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
FINMA guidance 08/2023 Staking	**Conten** • Staking services and the associated requirements of the DLT bill (BBl 2020 7801 - Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology) have recently become a growing segment in the financial market. FINMA guidance 08/2023 addresses and clarifies relevant issues. **Definitions** • Staking = The process of blocking native crypto assets at the staking address of a validator node in order to participate in a blockchain validation process based on a proof-of-stake consensus mechanism. • Staking rewards = Rewards earned by participants of crypto assets. • Proof-of-stake mechanism = Validation process of individual transactions (blocks) in the blockchain by a random draw of a participant, whereby the probability of the draw increases for users with a high number of tokens assigned to the validator node. • Node A node („network node") is any computer that connects to the crypto-currency of its choice by downloading the open source software. In principle, it serves as a connection point for data transfers in interaction with other participants (nodes) in the network around the world, which together form the backbone of the blockchain. **Risks of staking** 1. Technical risks and penalties System or connection problems (e.g. interruption of the internet connection) can occur during the staking process, which can lead to failure of the proof-of-stake mechanism and result in the crypto assets being slashed, i.e. a deduction is made as a penalty. 2. Counterparty risk due to bankruptcy The legal situation regarding the treatment of staked crypto assets in the event of the counterparty's bankruptcy has not yet been clarified. The corresponding risk is significantly increased if the assets are held in custody by institutions domiciled abroad. 3. Market risks The redemption of staked crypto assets can be delayed by a lock-up/exit period as part of the unstaking process. In a volatile period, it may not be possible for the holder to sell the assets at the right time. In certain blockchains (e.g. Ethereum), these periods can also be extended by lengthening the lock-up period as the number of unstaking orders rises. **Treatment under supervisory law** 1. Segregation under bankruptcy law (Art. 242a para. 2 SchKG) Bankruptcy protection does not apply to crypto assets used for staking if the custodian carries out staking for its own account, i.e. if it carries out proprietary trading in accordance with Art. 1a lit. b of the Banking Act (BA). It is more difficult if the staking is carried out by a third party, but on behalf of and for the account of the owner. In this case, the specific staking mechanism must be assessed on a case-by-case basis. Mechanisms that do not prescribe a lock-up period are unproblematic, as in this case the crypto assets are available to the owner at all times. 2. Licence requirements under banking law (Art. 1a and 1b BA in conjunction with Art. 5 and 5a Banking Ordinance (BO)) It should be noted here that individual custody qualifies as an activity of a financial intermediary under the Anti-Money Laundering Act (AMLA); such service providers must join a self-regulatory organisation for the purposes of money laundering supervision.	• Ensure clear instructions for the staking client, including the crypto-based assets required for staking and transparent information on all opportunities and risks. • Review operational risks (organisation of business continuity management) of staking services on an ongoing basis and adjust if necessary.	**Published on 20 December 2023**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Indirectly or partially affected

Proposed or enacted changes

Topic	Background and changes	Action required	Timeline
	Accounting treatment • In a staking chain, the crypto-based assets to be staked are passed on by the service provider with the customer relationship to one or more third parties who operate the validator node and hold the withdrawal keys. If an authorised institution delegates the operation to a third party, it has a claim against this third party for accounting purposes, which can either be recognised as a claim against the third party or as a deposited security in the sense of a claim held in trust (Art. 16 para. 2 Banking Act). This requires a valid fiduciary agreement with a crypto-specific fiduciary mandate. • In the case of direct staking, the service provider operates the validator node itself or outsources its operation to a technical service provider, but at least holds the withdrawal keys for the redemption of the customer's staked crypto-based assets itself. Segregation within the meaning of Art. 16 para. 2 Banking Act therefore does not apply.		

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Indirectly or partially affected

Proposed or enacted changes

Topic	Background and changes	Timeline
Revision of the ordinance on the tax deductibility of contributions to recognised forms of pension provision (BVV 3) Subsequent purchases in pillar 3a	**Content** • On 22 November 2023, the Federal Council submitted the revision of the ordinance on the tax deductibility of contributions to recognised forms of pension provision (BVV 3) for consultation on the introduction of purchases in pillar 3a. In future, it should be possible to subsequently close contribution gaps in pillar 3a with tax-deductible purchases within up to 10 years. This is intended to strengthen tax-privileged personal pension provision and provide additional support for the Swiss social security system. **Key changes to Art. 7a BVV 3** • Deductible contributions to Pillar 3a in accordance with Art. 7 BVV 3 can now also be made in the form of purchases. Anyone who has an income subject to old age and survivors' insurance (OASI) in Switzerland and is therefore entitled to make a contribution to a tied pension plan in the year of purchase is eligible to make a purchase. It is also assumed that the eligible person has not exhausted the maximum permissible amount in the absolute period of 10 years preceding the purchase year. Gaps in contributions dating back longer than this can no longer be closed. • Gaps can only be closed for those contribution years in which the person making the provision also fulfilled the requirements for paying pillar 3a contributions. The purchase potential results from the sum of the contribution gaps of the past 10 years that are subsequently eligible for adjustment. The maximum amount minus the contributions paid must be calculated separately for each contribution year. • Purchases can be made cumulatively with the maximum annual contributions and at the same time presuppose that the insured person has exhausted these in the year in which the purchase is to be made. Thus, Art. 7a para. 1 lit. c BVV 3 does not permit a purchase to be made instead of the ordinary contribution. • Purchases may be made annually and therefore in any contribution year, provided that the requirements of Art. 7 BVV 3 are met. • According to Art. 7a para. 2 BVV 3, the purchase payment may not exceed 8 per cent of the upper limit of CHF 88,200 in accordance with Art. 8 para. 1 Federal Law on Occupational Retirement, Survivors' and Disability Pension Plans (BVG) and is thus limited to the amount of the deduction according to Art. 7 para. 1 lit. a BVV 3. • The contribution gap for a contribution year may only be closed with a single purchase. Multiple annual purchases may therefore not be made to close a single gap. • Furthermore, the purchase entitlement requires that the retirement benefit pursuant to Art. 3 para. 1 BVV 3 has not yet been drawn. The insured person therefore forfeits the opportunity to make subsequent purchases into Pillar 3a when the retirement benefit is drawn. On the other hand, a purchase is still possible within five years of reaching regular retirement age, provided the insured person is still working. **Summary of prerequisites** • Contribution entitlement in the purchase year was utilised in full (maximum amount). • Contribution gap to be closed is no more than 10 years old. • Contribution entitlement for the gap year existed and was not fully utilised • Purchase payment does not exceed CHF 7065.00. • Contribution gap for the specific contribution year has not already been partially closed with a previous year's purchase payment. • OASI pension has not yet been drawn. **Carrying out the purchase** A purchase must be applied for in writing to the pension fund and reviewed by it. The application must contain the following: • Confirmation that the ordinary contribution has been paid in full in the current contribution year. • Confirmation that the contribution gap for the specific year has not already been closed by purchases made in previous years. • Confirmation from pension beneficiaries who have reached the age of 60 that no retirement benefits have been drawn to date. **Tax impact** • The Federal Tax Administration anticipates an estimated annual shortfall in income tax revenue for the cantons and municipalities of approximately CHF 200-450 million and a shortfall in direct federal tax of CHF 100-150 million.	**Consultation period runs until 6 March 2024**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

▶ Part 2

Current regulatory projects

Content

- Climate disclosures in Switzerland/ESG
- Transparency register for beneficial owners (BO)
- Operational risks and resilience – banks

Current regulatory projects

Topic	Background and changes	Action required	Timeline
Climate disclosures in Switzerland Federal Council's ordinance on mandatory climate disclosures for large companies of 23 November 2022 (VO BR) Basis: Recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) for large companies Environmental, Social and Governance (ESG)	**FINMA Guidance 01/2023: Developments in the management of climate risks (24 January 2023)** • In the guidance, FINMA draws attention to relevant developments in the area of climate-related financial risk management. The supervisor reiterates its expectation that supervised institutions establish an appropriate climate risk management framework based on recognised practices. Further developments will continue in line with relevant international developments. • International standard-setting bodies are developing concrete recom- mendations and guidance on dealing with climate risks, and expect banks and insurance companies to manage climate risks effectively - in the same manner as applies to other risks - including in areas such as governance, risk management or disclosures. • For its part, FINMA will continue to develop its supervisory practice for assessing the management of climate-related financial risks. In doing so, it will take into account the work of the standard-setting bodies. Where appropriate and necessary, FINMA will specify what it expects from supervised institutions in terms of climate risk management. • VO BR: Obligation for public companies, banks and insurance companies that employ at least 500 people and have a balance sheet total of at least CHF 20 million or sales revenue of more than CHF 40 million to report publicly on climate issues in accordance with internationally recognised recommendations of the TCFD. • The TCFD recommendations represent an internationally recognised standard. In addition to the eleven recommendations, cross-sectoral and sector-specific guidance must also be taken into account during implementation. Implementation is an iterative process. • The TCFD recommendations cover four thematic areas i) Governance; ii) Strategy; iii) Risk Management and iv) Metrics & Targets. • SBA Guidelines of June 2022 for its member institutions: - "Guidelines for the financial service providers on the integration of ESG-preferences and ESG risks into investment advice and portfolio management" - Q&A document (investment advice and asset management) on the guidelines dated 12 January 2023 - "Guidelines for mortgage providers on the promotion of energy efficiency" • ESG: Corporate social responsibility (CSR) standards that go beyond a company's financial reporting; includes an evaluation of corporate social responsibility in the sense of a voluntary contribution by business to sustainable development that goes beyond the legal requirements (also part of corporate governance and sustainability). • ESG relates, among other things, to a large-scale European regulatory package that defines the framework for dealing with sustainable investments: - Regulation on the establishment of a framework to facilitate sustainable investment ("taxonomy") with the aim of enabling uniform criteria for classification of activities ("what is environmentally sustainable?"). - Regulation on disclosure of information on sustainable investments and risks with obligation for financial institutions in the EU to comply with various disclosure obligations. - Regulation on low carbon benchmarks and positive carbon impact benchmarks with the aim of creating standards for these benchmarks. - Adapt MiFID II and IDD by taking ESG factors into account: ESG preferences of clients are to be included in suitability and appropriateness assessments (sustainable investment).	• Establish adequate climate risk management in line with the risk profile of the supervised institutions (FINMA expectation). • Proactively address the recommendations and guidance provided by international bodies as well as best practices in the market (FINMA expectation). • Supervised institutions should further develop instruments and processes (where necessary) (FINMA expectation). • Revise corporate strategy and planning (climate issues as a strategic component). • Analyse the governance of the company in relation to requirements under the Federal Council's ordi- nance (VO BR) and ESG regulation: top-down principle. • Define a "TCFD" project mandate (binding for all organisational units) with an initial GAP analysis in relation to TCFD recommendations. • Create an action plan with defined tasks, targets and responsibilities. • Analyse investment/financial products with an emphasis on CSR standards. • Provide employee training on ESG criteria and CSR standards and introduce motivational factors (part of the target agreement). • Consider communication to clients and other stakeholders. • Integrate sustainability risks in internal risk management.	**Entry into force:** • VO BR on 1 January 2024 • Publication of 1st climate disclosures in accordance with VO BR by the end of 2024 at the latest • EU regulations: between 2020 and 2022 • Entry into force of the SBA guidelines for member institutions: 1 January 2023

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Indirectly or partially affected

Current regulatory projects

Topic	Background and changes	Timeline
Creation of a transparency register for beneficial owners (BO)	**Federal Council mandate and background** • During its meeting on 12 October 2022, the Federal Council instructed the Federal Department of Finance (FDF) to draft a bill on increased transparency and easier identification of the beneficial owners of legal entities by the second quarter of 2023. In this way, it wishes to strengthen prevention and prosecution in the area of financial crime, and in turn the integrity and reputation of Switzerland as a financial centre and business location. • On 30 August 2023, a draft bill for the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners went out for consultation. The goal is to submit the dispatch to parliament in 2024. • Current legal basis is Art. 697j et seq. CO („ Register of beneficial owners"); inserted pursuant to the Federal Act of 12 December 2014 for implementing the Revised Financial Action Task Force (FATF) Recommendations. • Purpose: Alternative to the abolition of the bearer share (insufficient transparency on the beneficial owner). • Assessment: The implementation of the previous legal requirements is insufficient. **Objective of the transparency register** • Increase transparency to facilitate identification of beneficial owners of legal entities. The bill aims in particular to introduce a central register for the identification of beneficial owners and new duties for risk-based updating of information on effective ownership. • The register shall be accessible to relevant authorities, but not to the public. • The Federal Council places great emphasis on combating financial crime and this bill marks a further step towards strengthening the Swiss system. At the same time, it is implementing a measure of its 2021-2024 anti-corruption strategy. • Beyond the national level, Switzerland has participated in the establishment of a global identifier system for financial market actors (GLEIF) to improve the quality of financial data and better assess systemic risks. The international legal entity identifier system (LEI) can also help to clearly identify companies and detect systemic risks by using information from the register of beneficial owners. • In addition, the Global Forum on Transparency and Exchange of Information for Tax Purposes has issued recommendations on the transparency of beneficial owners of legal entities and regularly evaluates the implementation of these. Compliance with international standards is a strategic goal of the Federal Council, particularly with regard to the EU lists of countries with increased money-laundering risks and those that are non-cooperative for tax purposes. **Key elements** • The introduction of a federal register for the beneficial owners of legal entities, to be maintained by the FDJP and accessible to the competent authorities, financial intermediaries, advisors and lawyers, in order to fulfil due diligence duties under anti-money laundering law. • The establishment of a control body attached to the FDF to safeguard the quality of the register. • New duties for companies to identify, verify and update their beneficial owners; shareholders and beneficial owners must cooperate in the fulfilment of these duties. • The introduction of obligations to notify the company and relevant registers; these apply to directors, managers, partners and shareholders acting in a fiduciary capacity. **Adressees of the law** • Legal entities under Swiss law (public limited companies (AG/SA), limited liability companies (GmbH/SARL), SICAVs/SICAFs, cooperatives, foundations and associations required to be entered in the commercial register). • Legal entities domiciled abroad that have a close connection to Switzerland and pose special risks (e.g. real estate ownership, actual management in Switzerland or operation of a branch). **FATF recommendation of March 2022** • Financial Action Task Force (FATF) adopts the revised recommendation on transparency and beneficial ownership of legal entities. Implementation of this will be assessed for all member countries as part of the next country review. Switzerland is a member of the FATF. In 2020, Switzerland already received recommendations to further improve the transparency of beneficial owners of legal entities. It is expected that Switzerland will be reviewed by 2027.	**Draft bill according to Federal Council mandate by 2nd quarter of 2023** Entry into force from 2024

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Current regulatory projects

Topic	Background and changes	Timeline
	Judgment of the ECJ on the anti-money laundering directive (right of inspection and privacy rights - 11/2022): • **Ruling:** The provision whereby the information on the beneficial ownership of companies incorporated with- in the territory of the Member States is accessible in all cases to any member of the general public is invalid. • **Facts of the case:** In accordance with the anti-money laundering directive, a Luxembourg law adopted in 2019 2 established a "Registre des bénéficiaires effectifs" (register of beneficial ownership) and provides that a whole series of information on the beneficial owners of registered entities must be entered and retained in that register. Some of that information is accessible to the general public, in particular through the Internet. That law also provides that a beneficial owner may request Luxembourg Business Registers (LBR), the admin- istrator of the Register, to restrict access to such information in certain cases. • **Reasons:** According to the Court, access by all members of the public to information on beneficial owners constitutes a serious infringement of the fundamental rights to respect for private life and to protection of personal data enshrined in Articles 7 and 8, respectively, of the Charter. Indeed, the information divulged makes it possible for a potentially unlimited number of persons to become aware of the material and financial situation of a beneficial owner. Public access to the register may entail considerable risks for the beneficial owners. It is not ensured that the information is used exclusively to combat money laundering and terrorism financing. Providing access for everyone under the amending directive goes beyond the objective and is not compatible with the European Charter of Fundamental Rights. Source: European Court of Justice (ECJ), 22 November 2022 - C-37/20, C-601/20 **Assessment of the Transparency Register Act/ "Swiss finish" and legal comparison with the EU** • Message for the Swiss legislator on the Transparency Register Act and the right of inspection: Restriction to competent authorities. • It can be assumed that direct access to the transparency register will also be granted to the Federal Tax Administration (SFTA) and cantonal tax authorities (analogous to Sec. 23 para. 1 of the German Anti-Money Laundering Act ("Geldwäschereigesetz"): access without reason for authorities, incl. the Federal Central Tax Office and local tax authorities). • There are no plans to grant access to private (financial) companies and journalists (in contrast to Germany: staggered access, i.e. financial intermediaries with the respective obligations are granted access if they can demonstrate that they are fulfilling their due diligence obligations; or other persons, such as journalists, upon presentation of a journalist's ID and proof of a justified interest, e.g. ongoing or planned research in the area of money laundering and terrorist financing; incl. research in the area of tax evasion pursuant to Sec. 370 of the German Tax Code ("Abgabenordnung") as a predicate offence to money laundering).. **Areas of action** • Follow the ongoing legislative process and interim announcements (www.admin.ch); inspect the draft legislation. • Ensure internal transparency of the beneficial owners (control holders in the case of public limited companies or limited liability companies).	

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Directly affected	Directly affected

Current regulatory projects

Topic	Background and changes	Timeline
"Operational risks and resilience – banks" Revision of FINMA Circular Creating the necessary transparency with regard to operational risks and resilience	**Preliminary remarks** • Global risks and their effects, such as developments in information and communication technology (ICT) and digitalisation, especially with storage of client identifying data (CID) in cloud solutions, place high demands on the data security of data controllers (with reference to the revised FADP and the DPO; in force on 1 September 2023). • Technological developments are causing risks in the financial sector to shift to the disadvantage of banks and other financial intermediaries. • The regulator requires a preventive review of security standards to protect against data loss or data manipulation (cyber risks) in order to adequately counter these operational risks ("operational resilience"). Defining operational resilience and risk assessment • FINMA defines operational resilience as the ability of financial institutions as a whole to prevent, adapt to, respond to, recover and learn from operational disruptions. • Operational disruptions and the non-availability of critical business services have the potential to cause widespread damage to consumers and market integrity, threaten the viability of institutions and cause instability in the financial system. Main points 1) Proportionality principle: Implementation in individual cases depending on the size, complexity, structure and risk profile of the institution. 2) Overall management of operational risks as part of the institution-wide risk management: The board of directors approves the basic principles for the management of operational risks relevant for the institution and monitors their application. This includes: • Management of information and communication technology (ICT) risks: Requires a high level of expertise from all members involved a) Cyber risks b) Risks relating to critical data c) Risks resulting from the design and implementation of BCM d) Risks from cross-border service business **Areas of action** Board of directors: • The BoD is responsible for defining an ICT strategy (technological orientation and developments) and monitoring its effectiveness.. Executive board: • The executive board implements the ICT strategy, manages the ICT risks and ensures that sufficient resources are available for this purpose. It is also responsible for ensuring that the reliability, integrity and availability of the ICT used are guaranteed. Internal reporting and content – margin no. 41 et seq. OpRisk Circular: • External factors such as recognised loss events of other institutions, changes in the security situation (e.g. as a result of environmental influences, cyber attacks or terrorism) or changes to the regulatory requirements must be taken into account. A summary overview of the effectiveness of the key controls and the inclusion of emerging operational risks is required. • Results from the application of additional instruments and methods according to margin no. 33 OpRisk Circular such as systematic collection and analysis of internal loss data and relevant external events are ad- ditionally included in internal reporting. ICT (operations and maintenance) – margin no. 53 et seq. OpRisk Circular: • An inventory of all components of ICT (hardware, software and location of critical data) shall be kept and made available in real time; it shall be updated regularly. Processes, procedures and controls shall be in place to ensure the confidentiality, integrity and availability of the ICT environment (including backup and recovery). Incident management – margin no. 58 et seq. OpRisk Circular: • Procedures, processes and controls should be in place to reduce the risk of security incidents. To this end, roles and responsibilities for handling incidents must be defined and ICT incidents must be linked with the processes for business continuity management and the disaster recovery plan.	**Entry into force: 1 January 2024** • Transitional periods: With regard to ensuring operational resilience, there is generally a transition period of two years for the addressees a (see references in Circular 2023/01, margin no. 113). For selected requirements (e.g. in relation to the inventory), there is a transitional period of one year from entry into force.

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Not affected

Current regulatory projects

Topic	Background and changes	Timeline
"Operational risks and resilience - banks (2)"	**Cyber risk management - margin no. 61 et seq. OpRisk Circular** • To manage the necessary technological advances, cyber risks must be transparently integrated into the operational risk inventory. For this purpose, an annual cyber risk report should be made to the executive board (effectiveness of controls, cyber events), taking into account the minimum requirements within the framework of the internal control system (ICS). This includes the identification of cyber risks based on the IT inventory and the business process portfolio as well as the implementation of procedures and controls for system monitoring to detect and respond to cyber attacks (incl. duty to report cyber attacks to FINMA and corresponding follow-up analyses). • Planning must include procedures to restore business operations and to respond to cyber attacks. This includes, but is not limited to, mandatory cyber risk awareness programmes for employees as well as periodic vulnerability assessments and penetration tests. **Critical data risk management - margin no. 71 et seq. OpRisk Circular** • The revised circular expands the focus on confidentiality in the context of CID to include the dimensions of integrity and availability of critical data in general. This is in line with the Basel Committee on Banking Supervision (BCBS). • Critical data describes data that requires special protection. It is the responsibility of the bank to classify the data according to risk. • It is recommended to manage critical data in line with a defined and documented data strategy. • To comply with the requirements on confidentiality, integrity and availability of critical data, first the processes, controls, roles and responsibilities in relation to critical data must be defined. - Comply with the requirements for confidentiality, integrity and availability of critical data. - Critical data stored outside Switzerland must be protected. - Incidents must be reported immediately to FINMA. - Due diligence (DD) must be exercised when selecting service providers with access to critical data; this means establishing DD criteria and ensuring periodic review. **Business continuity management (BCM) - margin no. 83 et seq. OpRisk Circular** • The previously binding BCM requirements were carried over with minor adjustments. BCM requirements must be updated in the event of significant relocations. Before the new Circular enters into force on 1 January 2024, the BoD must approve the organisation's objectives on the revised topics of "continuity objectives" (also called "tolerances for disruption") and "critical functions".. **Operational resilience - margin no. 101 et seq. OpRisk Circular** • FINMA defines operational resilience as the ability of financial institutions as a whole to prevent, adapt to, respond to, recover from and learn from operational disruptions. Operational disruptions and the unavail- ability of critical business services have the potential to cause widespread harm to consumers and market integrity, jeopardise institutions' profitability and cause instability in the financial system. • The following aspects support operational resilience: - Focusing with a top-down view (top=BoD) on the most strategic operations (referred to in the circular as "critical functions"). - Identification of critical functions* and the associated tolerances for disruption are to be approved (annually) by the BoD. * Kritische Funktionen: Prozesse, Dienstleistungen und die für ihre Erbringung erforderlichen Ressourcen, deren Unterbrechung den Fortbestand des Instituts oder seine Rolle auf dem Finanzmarkt gefährden würde.	**Entry into force from 2024**

Banks and securities firms	Asset management institutions	Portfolio managers and trustees
Directly affected	Indirectly or partially affected	Not affected

Contact us

For further information on this topic or about our services, please contact us via our Regulatory & Compliance Financial Services Team:

Zurich

Susanne De Zordi
susanne.dezordi@bdo.ch

Dr. Detlev M. Basse
detlev.basse@bdo.ch

Geneva

Patrick Cattin
patrick.cattin@bdo.ch

Taulant Avdija
taulant.avdija@bdo.ch

BDO Ltd
Schiffbaustrasse 2
8031 Zurich
Tel. 044 444 35 55

www.bdo.ch

BDO Ltd

BDO Ltd is one of the leading audit, business services and advisory firms in Switzerland. We offer services in our core areas of expertise: audit, financial services, business services and outsourcing, tax and legal advisory, and management consulting. With 36 offices in Switzerland, our firm's network offers the most extensive coverage in the industry. For BDO's people – around 1,600 professionals – close links and expertise are the key to successful and lasting relationships with our clients. Our first fully digital office enables SMEs to also automate simple and standardised processes. BDO Ltd audits and advises industrial and service sector companies, including SMEs, listed companies, public authorities and non-profit organisations.

For clients with an international focus, BDO draws on a global organisation spanning more than 160 countries. BDO Ltd has its head office in Zurich and is an independent, legally separate Swiss firm belonging to the international BDO network, whose head office is in Brussels (Belgium).