Banking Act

Last change: 23.08.2026

PDF generated on: 05.10.2026

ONLINE COMMENTARY
THE OPEN ACCESS
LEGAL COMMENTARY

TABLE OF CONTENTS

Art. 1b BA 5

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 1b BA

A commentary by Tamara Teves / David Meirich

SUGGESTED CITATION

Tamara Teves/David Meirich, Commentary of art. 1b BA, in: Nina Reiser/Beat Brändli (ed.), Online Commentary of the Banking Act

Short citation: OK-Teves/Meirich, art. 1b BA N. XXX.

Article 1b Innovation funding

[1] The provisions of this Act shall also apply to persons who are primarily active in the financial sector,

and:

a. accept deposits from the public up to CHF 100 million or crypto-based assets designated by the Federal Council on a professional basis or who publicly advertise as doing so; and

b. who neither invest nor give interest on these deposits from the public.

[2] The Swiss Federal Council may adjust the amount mentioned in (1), taking into account of the competitiveness and innovative capacity of Switzerland as a financial center.

[3] Persons as per (1) shall specifically:

a. precisely define their scope of business and provide for an administrative organization in keeping with their business activities;

b. dispose of an adequately endowed risk management and effective internal controls, which ensure the adherence to legal regulations and company-internal policies (Compliance);

c. dispose of adequate financial means;

d. ensure that the persons in charge of administration and management enjoy a good reputation and thereby assure an irreproachable conduct of business operations;

4 The following provisions shall remain applicable:

a. The accounting for persons as per (1) shall base itself exclusively on the provisions of the Swiss Code of Obligations (CO)s (CO).

b. Persons as per (1) shall have their annual financial statements and, if necessary, their consolidated financial statements audited in accordance with the provisions of the CO; Article 727a(2)-(5) CO shall not apply.

c. Persons as per (1) shall arrange for an audit firm licensed by the Federal Audit Oversight Authority under Article 9a(1) or (4bis) of the Auditor Oversight Act of 16 December 2005 with an audit in accordance with Article 24 of the Financial Market Supervision Act of 22 June 2007 (FINMASA).

d. The provisions on privileged deposits (Article 37a) and on immediate payout (Article 37b) shall not apply to deposits from the public or crypto-based assets as designated by the Federal Council held by persons as per (1); depositors shall be informed of this prior to making the deposit.

5 Under special circumstances, FINMA may also declare (1)-(4) applicable to persons who accept deposits from the public on a professional basis in excess of CHF 100 million or who publicly advertise as doing so but who neither invest nor grant interests on these funds and who ensure the clients' protection with special precautions.

[6] If the threshold of CHF 100 million is exceeded, FINMA must be notified within 10 days and a license application in accordance with Article 1a shall be submitted within 90 days. (5) shall remain applicable.

CONTENT

I. Introduction 11
II. Licensing Procedure 12
A. Preliminary Review 12
B. Application Review 14
C. Licensing Decision 16
III. Scope of Application (Para. 1 and 2) 17
A. Acceptance of Public Deposits (Para. 1, letter a) 17
B. Collective Custody of Crypto-Based Assets (para. 1(a)) 17
C. Prohibition on Investment and Payment of Interest (Para. 1, let. b) 18
D. Adjustment of the Threshold for Public Deposits by the Federal Council (para. 2) 20
IV. Licensing Requirements (Para. 3 and 4) 20
A. Scope of Business (Para. 3(a)) 20
1. General Provisions 20
2. Custody of Public Deposits and Crypto-Based Assets (para. 3(a)) 23
a. Custody of Public Deposits 23
b. Monitoring of the Threshold for Public Deposits (para. 6) 25
3. Custody of Crypto-Based Assets 26
B. Appropriate Administrative Organization (para. 3(a)) 27
1. Legal Form, Registered Office, and Place of Business 27
2. Governing Bodies 29
3. Infrastructure and Personnel 30
a. Business Premises 30
b. Human Resources 30
c. Technical Infrastructure 31
4. Outsourcing 31
a. Outsourceability 31
b. Materiality 32
c. Inventory 33
d. Risk Analysis 33
e. Selection, Instruction, and Oversight of the Service Provider 33
f. Audit and Supervision 34
g. Outsourcing Agreements 34
h. Reporting 36
i. Group-related matters 36
j. Responsibility and Security 36
k. Outsourcing Abroad 36
l. Conditions and Exceptions 37

C. Corporate Governance: Risk Management, Internal Controls, and Compliance (para. 3(b)) ... 37
1. Basic Principles ... 37
2. Independent Control Functions ... 39
a. Responsibilities ... 40
b. Inventory ... 40
c. Identification ... 41
d. Risk Tolerance ... 41
e. Employee Training ... 42
f. Control ... 42
g. Reporting ... 42
h. ICT Risks ... 43
a. Strategy and Governance ... 43
b. Change Management ... 43
c. ICT Operations ... 43
d. Incident Management ... 44
i. Cyber Risks ... 44
j. Risks to Critical Data ... 46
k. Business Continuity Management ... 47
l. Risks Arising from Cross-Border Service Activities ... 49
m. Operational Resilience ... 49
4. Anti-Money Laundering Unit ... 50
5. Documentation and Processes ... 51
6. Avoidance of Conflicts of Interest ... 52
D. Financial Requirements (para. 3(c)) ... 52
1. Business Plan ... 52
2. Liquidity ... 54
3. Minimum Capital ... 54
E. Guarantee (para. 3(d)) ... 55
F. Financial Reporting and Auditing (para. 4, lit. a, b, and c) ... 58
G. Disclosure Requirements (para. 4, letter d) ... 59
V. Special Cases (including paras. 5 and 6) ... 60
A. Possible Increase in the Threshold for Public Deposits by FINMA (paras. 5 and 6) ... 60
B. Combination with Other Licensing Categories ... 60
C. Consolidated Supervision ... 61
D. Cross-Border Matters ... 64
1. Foreign Business (outbound) ... 65
2. Foreign Control ... 66
3. Representative Offices (inbound) ... 66
VI. Changes to Authorization ... 68

VII. Approval History 69
VIII. Further Development of Fintech Licensing 70
Bibliography 71
Materials 73

I. INTRODUCTION

The present Art. 1*b* was incorporated into the BankG by Parliament on June 15, 2018—as part of the provisions on **promoting innovation**—along with the Financial Services Act and the Financial Institutions Act. All of these provisions on promoting innovation entered into force on January 1, 2019. 1

The **fintech sector** is subject to constant change. Accordingly, business models in this sector are also evolving. To take this into account, the licensing category under Art. 1*b* para. 1 of the BankG is not limited to specific fintech business models or to the fintech sector as such. Although the new regulation was primarily intended to lower market entry barriers for fintech companies, the provision is broadly worded and applies generally to all persons operating in the financial sector. Thus, in principle, companies outside the fintech sector may also obtain a license under Art. 1 *b* of the BankG, provided they meet the statutory requirements. The broad scope of application is also reflected in the title of the statutory provision ("Promotion of Innovation"). Despite this broad scope, however, the focus in practice remains on the fintech sector. A specific innovation is not required within the framework of this licensing category. 2

In some cases, the business models of fintech institutions also require the **acceptance of public deposits** (so-called deposit-taking business). However, even after the introduction of the provisions on innovation promotion, the simultaneous conduct of lending business (and thus the interest margin business) is to remain the exclusive preserve of banks. For this reason, a fintech institution is not permitted to invest the funds it receives or to pay interest on them (see Art. 1*b*, para. 1, letter b, BankG). 3

Prior to the enactment of Art. 1*b* BankG, the commercial acceptance of public deposits was reserved exclusively for **banks**. Engaging in such activity without a banking license was a criminal offense (see Art. 46 para. 1(a) and Art. 49 para. 1(c) of the BankG). The fintech institutions specifically covered by this regulation provide banking-like services but operate outside the core business of banks. 4

In Switzerland, numerous services (including payment services as well as trading and individual custody of crypto-based assets) —provided their activities are not covered by other financial market laws—can be provided even without a license from the Swiss Financial Market Supervisory Authority 5

(FINMA), though they remain subject to anti-money laundering supervision by SROs. Thus, both certain payment services and the trading and individual custody of crypto assets can be offered under SRO supervision (currently, there are estimated to be around 200 crypto service providers and around 50 payment service providers under the supervision of SROs). This background should be taken into account when estimating the number of new service providers. The fintech licensing regime under Art. 1*b* of the BankG is thus aimed at a very specific business model profile: institutions that accept and transfer public deposits (customer funds) (payment services).

6 Compliance with the licensing requirements is monitored by FINMA as part of its ongoing supervision; FINMA is also responsible for imposing regulatory sanctions for misconduct, such as engaging in an activity requiring a license without one.

II. LICENSING PROCEDURE

A. Preliminary Review

7 For projects that could lead to a licensing procedure for fintech institutions (as is the case with banks and securities firms), a preliminary review. The **preliminary review** is intended to enable FINMA to familiarize itself with the basic features of the project and to conduct an initial regulatory assessment. This allows project initiators to receive early indications of any potential obstacles to authorization or to discuss key issues directly with FINMA.

8 When making initial contact, a **project proposal** must be submitted to FINMA, which should contain at least the following information:

- Business model and description of the activity requiring authorization;
- key figures behind the project (i.e., the individuals involved who may later serve as "guarantors");
- the project's financial resources and the source of funds (based on current figures);
- the planned organizational structure;
- if the project is part of a group: an overview of the group structure;

- any information regarding noteworthy events that could be relevant to the licensing process (e.g., proceedings against potential guarantors);
- a timeline;
- a power of attorney (if represented).

In summary, the project presentation should provide FINMA with an initial overview of the personnel, financial, and organizational structure of the project seeking authorization. 9

Upon receipt of the project presentation, FINMA will decide whether a meeting is warranted. Specific questions arising in the context of the licensing process, the answers to which are of particular importance to the main issue, may be addressed upon request as part of a **preliminary inquiry**. Project presentations must be submitted to FINMA's Fintech Desk in one of the official languages or in English. 10

If, as part of the preliminary review, FINMA concludes that the **eligibility for authorization** of the presented project is unlikely to be met—for example, due to a lack of sufficient financial resources, an unclear source of funds, the inability to ensure consolidated supervision, the lack of qualifications among the individuals involved to serve as future guarantors, or an insufficient presence in Switzerland, the submission of a license application is discouraged. In such cases, the project initiator may submit a new preliminary project proposal, provided that the issues raised during the meeting are adequately addressed and the necessary supporting documentation can be provided. 11

If FINMA is of the opinion that the project presented is likely to be eligible for approval, the applicant will be informed that it may submit the **licensing application**. The preliminary application is intended to be straightforward and cost-effective. Accordingly, it is not conducted as a formal administrative procedure concluding with an administrative decision. Rather, it can be understood as a preliminary assessment service provided by FINMA. 12

Preliminary assessments of licensing projects are subject to a fee. The **fee** is determined in accordance with the FINMA Fees and Charges Ordinance (FINMA-GebV). 13

B. Application Review

14 Following a successful preliminary review and upon submission of a licensing report, the corresponding **licensing application** may be submitted to FINMA.

15 In accordance with the dual supervision system, FINMA generally requires the applicant to submit a **licensing audit report** prepared by an audit firm with the appropriate authorization under Art. 9a of the AOA as part of the licensing procedure. Whether this is necessary is to be decided on a case-by-case basis; however, an audit report is required as a standard procedure. The audit reports from the various audit firms differ, in some cases considerably, in terms of quality (depth of audit) and cost, which the applicant must take into account when making a selection. The higher the quality of the report, the more helpful the audit report will be in the context of FINMA's further processing of the application. Ultimately, the duration of the licensing process depends on the complexity of the project as well as the quality and completeness of the application.

16 The **FINMA Guidelines** regarding the confirmations to be submitted by audit firms for applications for licensing as entities under Art. 1*b* of BankG are directed at audit firms with regard to licensing applications from fintech institutions to be newly established. The guidelines specify the required confirmations and the audit areas that must be covered by the audit firms, acting as licensing auditors, as a minimum during a licensing procedure. It does not preclude the possibility that audit firms may provide additional information or that FINMA may request further information and confirmations.

17 If an authorization audit is required —which is generally to be expected—the applicant must submit, along with the license application, a corresponding declaration of acceptance from the **license audit firm** as well as the completed questionnaire on the services of authorized audit firms.

18 FINMA is responsible for granting the fintech license. When reviewing such license applications, the supervisory authority assesses whether the intended business activities are subject to licensing and whether they are permissible under the fintech license. To facilitate the licensing process, FINMA has published guidelines for applicants. These guidelines specify, in particular, which documents must be submitted with the application.

The application must be drafted in an **official language or English**; however, the articles of association, the organizational regulations, and any other documents of a corporate law nature requiring approval must be submitted in a Swiss official language. FINMA does not accept articles of association or organizational regulations in English. In practice, these corporate law documents are generally drafted in two languages, which FINMA has accepted to date. If an application is submitted by a legal representative, the representative's power of attorney must be submitted. 19

Upon receipt of the application, FINMA will inform the applicant which FINMA employee is responsible for the **licensing procedure** and what additional information and documents may need to be submitted. 20

The supervisory authority may conduct the **licensing review** itself, as it does with all reviews, or have it conducted by others (see Art. 24 para. 1 of the FINMASA in conjunction with Art. 2(2) of the Financial Market Review Ordinance [FINMA-PV]). The review assesses whether the supervisory regulations are being complied with and whether the requirements are met or can be met in the foreseeable future (Art. 2 para. 1 FINMA-PV) . The review focuses in particular on the risks that the supervised entity may pose to creditors and to the proper functioning of the financial markets. Duplication of efforts in the review should be avoided wherever possible (para. 2 of Art. 24 of FINMASA). 21

FINMA ensures, in particular during the preliminary review, that fundamental **obstacles to authorization** are identified at an early stage. As soon as all relevant information and documents are available, FINMA reviews the application and decides whether authorization can be granted. The applicant has a duty to cooperate in providing the full facts of the case and demonstrating compliance with the licensing requirements. The requested license is granted if all licensing requirements are unambiguously met or can be met. 22

The **processing time** for the license application depends on the quality and complexity of the application as well as on communication with the applicants. For applications with a particularly strong foreign component—such as membership in a group that already includes foreign companies in the financial sector or the involvement of individuals who have come to the attention of foreign financial market supervisory authorities in the past—the response time of the relevant foreign supervisory authorities must also be taken into account. 23

24 **Factors**, that lead to lengthy licensing procedures may also occur in combination with one another:

- insufficient preparation of license applications (e.g., insufficiently specific description of the planned activities, inadequate or erroneous documentation);
- amendments to license applications by the applicants during FINMA's ongoing review (e.g., changes to the planned business activities and/or organization, changes to guarantors);
- numerous factors that increase complexity (e.g., questionable assurance that the relevant individuals will conduct business properly, prior rejection of an authorization application by the applicant by a foreign supervisory authority, unclear source of funds for financing the company, business or financing plans that are obviously unrealistic).

25 FINMA is currently examining the introduction of a **"fast-track" procedure** for well-prepared projects in which the risks are adequately addressed, so that these projects do not have to suffer from the high resource requirements associated with other license applications. This is intended to prevent the processing time for well-prepared, less complex license applications from being prolonged due to the resource requirements.

C. Licensing Decision

26 FINMA concludes the licensing procedure with a **licensing decision**. The decision is divided into the facts, the reasoning, and the operative part. While the facts section describes the applicant's organization, the reasoning section addresses compliance with the applicable licensing requirements. In the operative part, FINMA grants the license, which is generally subject to a suspensive condition regarding requirements and conditions that must still be fulfilled. Such requirements and conditions typically include the signing of employment or outsourcing agreements, the entry into force of directives and regulations, the existence of a legally valid signed copy of the organizational and operating regulations, as well as the existence of public documents regarding the resolution of the general meeting concerning the adoption of the draft articles of association, the pending election of the members of the board of directors, and the election of the auditor.

The license normally lapses if the conditions specified in the operative part of the decision are not met within a **one-year period** from the effective date of the decision and the applicant has not been entered in the Commercial Register as a person under Art. 1*b* of BankG. The authorization also becomes void if the applicant does not commence its newly authorized business activities (acceptance of public deposits and/or collective custody of crypto-based assets) within one year of this decision becoming final. An appeal against this authorization decision may be filed with the Federal Administrative Court within 30 days (Art. 54 para. 1 FINMASA in conjunction with Art. 33(e) of the Administrative Court Act (VGG)). 27

III. SCOPE OF APPLICATION (PARA. 1 AND 2)

A. Acceptance of Public Deposits (Para. 1, letter a)

Article 1*b* of BankG created a new licensing category for institutions that accept public deposits of up to CHF 100 million on a commercial basis without engaging in lending activities (the so-called "fintech license"). The Federal Council specified the licensing requirements as part of a partial revision of the Banking Ordinance (BankV), which entered into force on January 1, 2019. 28

B. Collective Custody of Crypto-Based Assets (para. 1(a))

With the entry into force of the Federal Act of September 25, 2020, on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology, effective August 1, August 2021, the **scope** of the fintech license was expanded. 29

Pursuant to Art. 1*b*, para. 1, subpara. a of the BankG, anyone who, on a commercial basis, accepts (collectively held) **crypto-based assets** designated by the Federal Council in accordance with Art. 5*a* of the Banking Ordinance (BankV). 30

Crypto-based assets are assets held in collective custody pursuant to Art. 16(1)^{bis}(b) of the BankG that, in fact or according to the intention of the organizer or issuer, serve to a significant extent as a means of payment for the purchase of goods or services or for the transfer of money or value, i.e., (hybrid) **payment tokens** (Art. 5*a* para. 1 BankV). 31

32 In the case of **collective custody**, the fintech institution is obligated to hold the payment tokens available for the customer at all times, whereby the tokens are allocated to a pool and it is evident (via blockchain or an internal register) what share of the pool's assets (i.e., a shared blockchain address) is attributable to the respective customer (Art. 16(1bis)(b) of the BankG).

33 The **individual custody** of payment tokens at an individual blockchain address within the meaning of Art. 16(1bis)(a) of the BankG therefore does not fall within the scope of the fintech license. This also applies to the custody of utility or investment tokens, i.e., tokens without a (hybrid) payment function.

34 A **license** under Art. 1*b* of the BankG may therefore be granted, on the one hand, to anyone who, on a commercial basis, accepts public deposits of up to CHF 100 million or crypto-based assets designated by the Federal Council, or publicly recommends the acceptance of such deposits or crypto-based assets, and, on the other hand, neither invests nor pays interest on these public deposits or crypto-based assets. The license is granted if the licensing requirements under banking law pursuant to Art. 1*b* of BankG are met.

C. Prohibition on Investment and Payment of Interest (Para. 1, let. b)

35 The **prohibition on investment and interest payments** within the meaning of Art. 1*b*, para. 1, let. b of the BankG effectively constitutes a prohibition on lending, i.e., a prohibition on lending activities. Consequently, only business models that do not engage in lending activities fall under the licensing category for fintech institutions. In these cases, the fintech license does not permit the interest margin business typical of banks.

36 The term **investment** must be understood very broadly in this context. Since the funds may not be invested, it is to be assumed that they are kept liquid at all times in the accounts of the relevant company (see Art. 14*f*, para. 2 BankV), forwarded to customers as intended in accordance with the agreement, or—if this is not the purpose or is not possible—repaid to the customers. Licensees are thus prohibited from engaging in the interest margin business reserved for banks and from generating profits from the difference between lending and deposit interest rates. The investment prohibition also means that deposits may not be invested (in the institution's own name and for its own account) in investment products.

In this regard, the investment and interest prohibition has the following **consequences** in practice: 37

- Fintech institutions may not grant their customers **loans** financed by public deposits. This also prohibits overdrafts and similar arrangements, as well as the intraday pre-financing of customer transactions (e.g., in the area of currency exchange or international payments) using public deposits. It must therefore be clarified on a case-by-case basis how relevant third-party service providers bill transaction and account maintenance fees as well as transaction pre-financing and margins—for example, whether the amounts deposited daily are financed from the company's own funds or from public deposits;
- **advances** from the company's own funds to settle customer transactions are also prohibited. Intraday advances from the company's own funds to settle customer transactions are possible only if the exception under para. 5(3)(a) of the Banking Ordinance (BankV) applies;
- **Foreign exchange forward transactions** generally cannot be offered by a fintech institution, as the associated capital and liquidity risks would require at least bank-like standards;
- the passing on of **negative interest rates** is permitted, but not the passing on of positive interest rates on current account deposits held with the SNB;
- **Credit products** in the crypto sector cannot be offered under a fintech license;
- **Custodial staking** is subject to a banking license, subject to the exceptions in Art. 5, Art. 5*a*, and Art. 6 of the Banking Ordinance (BankV), provided that staking results in de facto interest payments (staking rewards), which would conflict with the prohibition on interest payments; Alternatively, staking rewards could also qualify as utility fees, in which case custodial staking could also be offered by fintech institutions, provided that the requirements of FINMA Supervisory Circular 08/2023 "Staking" are complied with at all times with respect to the staked crypto-based assets. Legal doctrine holds that the payment of staking rewards to customers does not constitute a violation of the prohibition on interest payments.
- Bilateral **CFD trading platforms** generally qualify as bilateral organized trading systems (OHS) under the FinMIA. Classification as an OHS activity

means that a license as a bank, securities firm, DLT trading system, or trading venue (stock exchange, MHS) is required (para. 43 FinMIA). Consequently, a fintech license is not sufficient for this purpose.

D. Adjustment of the Threshold for Public Deposits by the Federal Council (para. 2)

38 The Federal Council may adjust the amount of **CHF 100 million**, taking into account the competitiveness and innovative capacity of the Swiss financial center (Art. 1*b* para. 2 BankG). In justified individual cases, FINMA shall also have the option to waive the CHF 100 million cap (Art. 1*b* para. 5 BankG).

39 In this context, the Federal Council announced in 2022 that it would review whether the **limit** on the acceptance of client funds at CHF 100 million should be maintained. Even though FINMA may, pursuant to Art. 1*b* para. 5 of the BankG, the limit creates uncertainty regarding how FINMA will ultimately decide. The criteria used by FINMA to grant an exemption in individual cases have not yet been published. Nor has the Federal Council yet commented more specifically on a possible adjustment of the threshold for public deposits within the framework of Art. 1*b*(2) of the BankG. We must therefore await the first instance in which this special provision is applied.

IV. LICENSING REQUIREMENTS (PARA. 3 AND 4)

A. Scope of Business (Para. 3(a))

1. General Provisions

40 The articles of incorporation or the **Organizational and Business Regulations** (OGR) must precisely define the **scope of business** in terms of both subject matter and geographical area (Art. 1*b*, para. 3, letter a, BankG; Art. 14*b*, para. 1, Banking Ordinance). The scope of business and its geographic extent must be commensurate with the applicant's financial resources and administrative organization (Art. 14*b*, para. 2, Banking Ordinance). Fintech institutions are prohibited from investing or paying interest on public deposits or crypto-based assets they have received (Art. 1*b*, para. 1, subparagraph b, BankG). It is not possible to include activities in the articles of incorporation or in the OGR "in advance."

The articles of incorporation or the OGR must reflect the **current activities** of a person under Art. 1*b* of BankG in detail ("precisely") in terms of subject matter, location, and personnel. Future activities generally depend on experience gained from other activities and must therefore be specified at the time of application and approved in advance by FINMA (see para. 8(2) of the Banking Ordinance). In this regard, the licensing process often requires that the relevant provisions in the articles of incorporation and the General Rules of Organization be specified in detail. 41

The application for authorization must include the following **general information**: 42

- Reasons and purpose for obtaining authorization as a person under Art. 1*b* of the BankG;
- a detailed description of the intended activities and organization, including the intended scope of business in terms of subject matter and geography, as well as the type of clientele targeted;
- an extract from the commercial register;
- an extract from the debt collection register (not older than 3 months) for the applicant;
- a declaration regarding pending and concluded proceedings (Form B1; signed and dated) for the applicant;
- information on group companies as well as holdings and/or other operations (branches or representative offices) of the applicant.

The required information regarding the **business activities, organization, and governance** of the applicant includes: 43

- a detailed description of business activities and related processes;
- a business plan, including a budget (balance sheet, income statement) for the next three fiscal years, with optimistic, realistic, and pessimistic scenarios;
- liquidity planning for the first fiscal year based on the pessimistic scenario of the business plan (on a monthly basis);
- Articles of incorporation, organizational regulations, and guidelines (regulations and directives) tailored to the business activities of a person as defined in Art. 1*b* of the BankG;

- Organizational chart identifying senior management and the FTE per organizational unit;
- Information on business premises (including submission of the lease agreement), infrastructure, and staffing;
- Organizational structure and regulations or directives concerning risk management, compliance, and the internal control system (including AMLA directives);
- Information and documentation regarding the outsourcing of activities (including a risk analysis, guidelines on objectives, requirements, responsibilities, and processes, an inventory of outsourced functions, and outsourcing agreements);
- Information and documentation regarding the management of operational risks (in particular, information and communication technology (ICT) risks, cyber risks, risks related to critical data, risks arising from the design and implementation of Business Continuity Management (BCM), and, where applicable, risks arising from cross-border service activities), ensuring operational resilience, and corresponding reporting;
- ICT planning, including details on the technical and operational readiness of individual applications and their criticality;
- an overview of the planned ICT and application landscape and internal system connections (including interfaces to third-party systems, guidelines regarding ICT systems and ICT security, as well as data storage and data security) upon commencement of operational activities;
- Description of how public deposits are held (separation from the company's own funds) and how compliance with the CHF 100 million threshold is ensured;
- if applicable: a detailed technical description of how crypto-based assets are custodied;
- detailed information regarding disclosures to customers in accordance with Art. 7*a* of the Banking Ordinance (BankV), specifically regarding risks and the absence of deposit insurance.
- A description of any conflicts of interest and related measures to protect clients from being disadvantaged in accordance with Art. 14*g* of the Banking Ordinance.

Institutions holding a fintech license may, in principle, employ a wide variety of business models (including crowdfunding, payment transactions—whether using traditional technologies or applications based on DLT/blockchain technology, etc.) . In practice, however, it has so far been shown that **payment service providers** in particular make use of this licensing category. 44

In addition to the activities that trigger the requirement for a license as a fintech institution, such an institution may in principle also provide ancillary services which, —when considered in isolation—would not trigger a licensing requirement. FINMA makes the provision of such an ancillary service—which, while not in itself triggering a licensing requirement, nevertheless increases the institution's risks—contingent upon the implementation of appropriate risk-mitigating measures (see Art. 14e para. 1 of the Banking Ordinance). If such measures are not implemented, or if the regulations governing fintech institutions do not allow for appropriate risk-mitigating measures, the provision of an ancillary service is incompatible with a license as a fintech institution. 45

2. Custody of Public Deposits and Crypto-Based Assets (para. 3(a))

a. Custody of Public Deposits

Fintech institutions must hold public deposits received (as defined in Art. 5 BankV) and collectively held crypto-based assets (as defined in Art. 5*a* BankV) **separately from their own funds** (Art. 14*f* para. 1 lit. a BankV) . In such cases, a limited audit within the meaning of Art. 727*a* of the Swiss Code of Obligations (CO) may be possible (Art. 14*f* para. 1 lit. b BankV *e contrario*) . According to a literal interpretation of Art. 14*f*, para. 1, subpar. a of the Banking Ordinance (BankV), it is not permissible to deposit customer funds into an account held by a third-party service provider, such as a payment processor without a banking license. Any necessary deposits with such payment processors would therefore have to be pre-financed from the fintech institution. 46

An **exception** to this separation is granted if the public deposits can be accounted for separately from the institution's own funds at all times and a proper audit is conducted in accordance with Art. 727 of the CO (Art. 14*f* para. 1 lit. b BankV). 47

However, companies are primarily obligated to forward the funds received in accordance with the agreement with the customers or—if this is not the pur- 48

pose or is not possible—to repay them to the customers. If immediate forwarding in accordance with the **customer agreement** is not possible or not provided for, the company may hold the deposits in custody. Although this "safekeeping" of deposits is not subject to any time limits, it is subject to certain conditions: The deposits must always be held in the best interests of the customers and may neither be invested nor earn interest. They must be held either as demand deposits at a bank or in the form of highly liquid assets.

49 The **consultation draft** of June 21, 2018, did not yet contain subparagraph b. The separate safekeeping of public deposits received was one of the main points of criticism during the consultation process, as it would have entailed considerable organizational and administrative burdens for FinTech institutions. In response to this criticism, the Federal Council provided for "accounting separation" in lit. b, subject to a regular audit in accordance with Art. 727 of the CO.

50 The holding of public deposits received is subject to the statutory **prohibition on investment and interest payments**. This means that, until they are repaid or transferred in accordance with their intended purpose, they must be held in a manner that that largely eliminates risks for customers. They must also be readily available so that they can be transferred for their intended purpose or refunded within a reasonable period of time. One option is to deposit the funds as demand deposits into a bank account with a bank or another entity pursuant to Art. 1*b* of the Banking Act (BankG). In this context, there should be no restrictive withdrawal limitations.

51 In accordance with the separation principle under Art. 14*f*(1)(a) of the Banking Ordinance (BankV), public deposits may be held as **demand deposits** at a bank or a fintech institution and/or as Category 1 **High-Quality Liquid Assets** (HQLA) pursuant to Art. 15*a* of the Liquidity Ordinance of November 30, 2012 (LiqV) (Art. 14*f* para. 2 BankV). Public deposits may therefore be held in the form of coins, banknotes, or central bank balances, or invested in certain marketable securities issued by specific debtors (such as central governments) without violating the investment prohibition. E-money institutions are generally not recognized in this context, unless there is a deposit insurance scheme or similar security for the funds received.

52 Public deposits must always be held in the currency of the **right to repayment** (Art. 14*f* para. 3 BankV). In particular, this also means that public de-

posits in collectively held crypto-based assets must be held as such (Art. 14*f* para. 4 BankV). The option to hold public deposits in HQLA may allow institutions to avoid negative interest rates. However, this gives rise to certain investment risks for customers, which may lead to higher minimum capital requirements.

Customers should, as far as possible, not be exposed to any additional risks, particularly **foreign exchange risks**. For this reason, public deposits accepted should only be held in the currency in which any claim for repayment exists. 53

The provisions on **privileged deposits** (Art. 37*a* BankG) and on immediate payment (Art. 37*b* of the BankG) **do not apply to deposits held with fintech institutions** (Art. 1*b*, para. 4, letter d of the BankG), as the legislature currently considers these provisions to be disproportionate. Consequently, fintech institutions are exempt from the obligation to join the self-regulatory body for deposit insurance and from the higher liquidity requirements applicable to **deposit insurance**. 54

b. Monitoring of the Threshold for Public Deposits (para. 6)

The **limit** on public deposits and collectively held payment tokens of CHF 100 million is mandatory (subject to Art. 1*b*, para. 2 and 5 of BankG). The license application must describe how compliance with the threshold of CHF 100 million in public deposits will be monitored. 55

Fintech institutions must therefore have documented procedures, controls (responsibilities, frequency), reporting (including forecasts), and other measures in place to monitor compliance with the threshold. In this context, a **tiered system of measures**—for example, at CHF 70, 80, 90, and 99 million—may be appropriate. Once a certain threshold is reached, technical restrictions must generally be put in place to ensure that no new public deposits are accepted and that existing ones are returned. Furthermore, coordination with FINMA must be established. 56

If several fintech institutions form a **financial group** pursuant to Art. 22 of the Banking Ordinance (BankV), the threshold of CHF 100 million must be calculated for the entire group (Art. 24*a* para. 1 BankV), unless the group companies are clearly independent of one another. This is intended to prevent this licensing category from being used for regulatory arbitrage in the area of 57

accepting public deposits. The aim is therefore to prevent arrangements designed to circumvent the CHF 100 million threshold.

3. Custody of Crypto-Based Assets

58 Crypto-based assets held in collective custody must be kept in Switzerland and in the form in which they were accepted (Art. 14*f*, para. 4, BankV) . Therefore, the power to dispose of private keys must, as a general rule, lie exclusively with fintech institutions or banks domiciled in Switzerland. Fintech institutions define in internal guidelines the handling of cryptographic keys that enable access to crypto-based assets. The internal guidelines must, among other things, a. govern the management and control of all required keys, i.e., their secure storage, provision, secure transmission, and the revocation of invalid or compromised cryptographic keys.

59 The **cryptographic keys** can, for example, be stored in a Hardware Security Module (HSM). With regard to the security of the HSM, the fintech institution should adhere to the U.S. government's Federal Information Processing Standard (FIPS) 140. This standard defines minimum security requirements for cryptographic modules in information technology products and is enshrined in Section 5131 of the Information Technology Management Reform Act of 1996.

60 In principle, it must be ensured that access to crypto-based assets is only possible via **multi- signature procedures**. One of the sub-keys must be managed by a member of executive management. The use of a private key must be preceded by the mandatory identification of the authorized user. For transactions exceeding a certain amount, the approval of a second member of executive management must be obtained. A simplified key management procedure may be provided for signing transactions involving small amounts. The use of private keys to sign transactions is subject to documentation requirements, compliance with which must be regularly verified as part of the internal control system (ICS).

61 Fintech institutions must also ensure that, in the event of the loss of partial keys (e.g., due to fire or similar circumstances), access to the crypto-based assets is possible via a **backup/recovery/master key** (*seed*). This key must be stored in a location separate from other private keys (e.g., in a safe at a finan-

cial services provider) . Access and exchange must be governed by an internal policy.

FINMA may, in individual cases, set an **upper limit** for crypto-based assets if this appears appropriate given the risks associated with the business. In doing so, the supervisory authority shall take into account, in particular, the function of the crypto-based assets, the underlying technologies, and risk-mitigating factors (Art. 4^{sexies} BankG). 62

Institutions that offer custody services for crypto-based assets must prepare a *Digital Asset Resolution Package* (DARP). The purpose of this document is to ensure that, in the event of the institution's bankruptcy, an external liquidator can promptly distribute the crypto-based assets to customers, thereby minimizing the effort and costs associated with their proper return. To this end, the DARP must contain the most important information for identifying and promptly securing the crypto-based assets, such as details regarding all persons required for the custody and trans crypto-based assets, including their functions and the associated instructions; details for accessing an up-to-date copy of the internal ledger, including the associated instructions; details regarding any third-party custodians, including the contact information of the persons at the third-party custodian responsible for the bank; etc. It must be ensured that the institution updates the DARP regularly. 63

B. Appropriate Administrative Organization (para. 3(a))

Fintech institutions must have an **administrative organization** that is appropriate to their business activities (scope of business and its geographical extent) (Art. 1*b* para. 3(a) BankG; Art. 14*b* para. 2 BankO). 64

1. Legal Form, Registered Office, and Place of Business

Fintech institutions must have the **legal form** of a stock corporation, a limited partnership with share capital, or a limited liability company and must have their registered office in Switzerland (Art. 14*a* BankV). The reason for this is to ensure proper supervision. 65

From a legal theory perspective, the general reference in Art. 1*b*(1) of the BankG can be interpreted to mean that, contrary to the text of the ordinance, a **cooperative** should be recognized as a permissible legal form. However, due to the difficulties associated with the requirement to maintain a minimum 66

share capital at all times, the cumbersome organizational and decision-making rules (in particular, the one-vote-per-share rule), and the share certificates —which may not be securitized as securities—this legal form is not suitable for operating a fintech institution.

67 The principal activity or actual management must be carried out in **Switzerland**, and the fintech institution must be effectively managed from Switzerland. The persons entrusted with management must be domiciled in a location from which they can effectively carry out their management duties (Art. 14*a*, para. 2, and Art. 14*c* of the Banking Ordinance).

68 The persons entrusted with **management** must reside near the applicant's registered office. It is required that they establish residence near the registered office or within Switzerland. According to current FINMA practice, it is expected that on each business day, at least some of the persons entrusted with management must be present at the registered office. This is intended to ensure that a Swiss fintech institution is not, in effect, managed from abroad.

69 According to current supervisory practice, in the case of guarantors holding a temporary short-stay residence permit (L permit), the risk of the **residence rights** lapsing must be addressed appropriately. The institution must identify this risk as part of its risk management and mitigate it through appropriate measures, namely reporting, delegation, and succession processes.

70 With regard to the **company name**, para. 1 of BankG stipulates that the terms "bank" or "banker," whether alone or in compound terms, in the company name, in the description of the business purpose, and in business advertising —for the protection of creditors—may be used only by institutions that hold a license from FINMA as a bank; this includes analogous terms in all national languages and all foreign languages, as well as, in principle, compound terms that suggest banking activities, are also included. Word combinations containing the elements "*bank*" or "*banking*" are therefore subject to scrutiny (including on the website, in the Official Gazette of the Swiss Confederation (OGR), or in the articles of incorporation). This even includes more creative variants such as "*non-bank*" or "*neo-bank*". In contrast, terms such as "*money accounts*," "*payment accounts*," "*payment services*," or similar word combinations should not pose any problems, since payment services do not necessarily have to be provided by a bank; membership in an SRO may be sufficient.

According to a analogous application of Art. 4*quater* of the BankG to fintech institutions, these institutions must therefore refrain from any misleading or intrusive **advertising**, both domestically and abroad, that refers to their Swiss registered office or to Swiss creditor protection mechanisms. 71

2. Governing Bodies

If the business purpose or scope of a fintech institution requires a specific governing body for general management, supervision, and control, this body must consist of at least three members (Art. 14*d* para. 1 Banking Ordinance) . Fintech institutions must generally have **administrative and management bodies**, and the body responsible for senior management, supervision, and control (board of directors) must comprise at least three members. At least one-third of the members of the board of directors must be independent of management (Art. 14*d* para. 2 BankV). 72

A member of the senior management body is considered **independent** if they: 73

- are not employed by the institution in any other capacity and have not been so employed within the last 2 years;
- have not been employed by the institution's audit firm as a senior auditor responsible for the institution within the last 2 years;
- do not maintain any business relationship with the institution that, due to its nature or scope, would lead to a conflict of interest;
- is not a qualified participant (within the meaning of Art. 3(2)(c^{bis}) of the BankG) of the institution and does not represent any such person; and
- in principle, is not in a close relationship (kinship, marriage, or cohabitation) with a member of the Executive Board.

In justified cases, FINMA may grant **exceptions** to the requirements for governing bodies (Art. 14*d* para. 4 Banking Ordinance). The separation of powers and functions is therefore not absolute. For example, FINMA may permit a fintech institution to have only an executive board but no board of directors. This exception is intended for very small institutions in the start-up phase. In particular, it is conceivable that *start-ups* might be granted temporary exemptions from the requirements regarding administrative organization until certain growth targets are reached; for example, independent board members 74

would be required only once gross revenue reaches CHF 1 million (and independent audit functions once it reaches CHF 1.5 million).

75 The definition of a "body" applies to **natural persons**. Legal entities are therefore not accepted as bodies. FINMA assesses whether members of the board of directors and executive management provide the so-called **assurance of sound business conduct**. This assessment is inherently person-specific and requires an evaluation of integrity, personal reputation, professional qualifications, experience, and conflicts of interest.

76 The required **supporting documentation** regarding the governing bodies includes:

- The composition of the governing body responsible for management, specifying the chairperson, vice chairperson, and members of any committees; and
- information on the composition, organization, and responsibilities of the executive management.

3. Infrastructure and Personnel

a. Business Premises

77 The applicant must have **suitable business premises** at its disposal. In terms of size, an office and a meeting room may be sufficient. If the applicant does not own the property, a (sub)lease agreement must be submitted. Information is required regarding access options and restrictions, the ability to lock the premises and furnishings, and the conduct of day-to-day business in compliance with data protection and banking secrecy regulations (e.g., a confidentiality agreement that ensures compliance with the confidentiality requirements applicable to the applicant in day-to-day business operations [particularly regarding the movement of people, mail, and physical ICT infrastructure]). Furthermore, the actual operational management of the company must be conducted from these business premises.

b. Human Resources

78 With regard to human resources, it is of central importance that the fintech institution has filled the necessary positions and can react quickly should additional **staff** be required for business operations. To this end, relevant infor-

mation must be provided, and the number of full-time equivalents (FTEs) in each area of activity should ideally be presented in a chart.

c. Technical Infrastructure

Fintech institutions generally do not have their own physical ICT infrastructure, with the exception of end devices and infrastructure for electricity, telephone, and internet connections. The majority of the **ICT infrastructure** is often cloud-based, which generally entails risks. 79

As part of the application, a more detailed description of the planned ICT architecture and the ICT components required for the planned activities is required. Accordingly, an ICT plan is also required that includes statements on the technical and operational **readiness** of the individual applications and their criticality. The fintech institution must provide information regarding the operational and technical readiness of its ICT applications. In a timeline, it must outline the status of implementation as well as the deployment of its planned applications and comment on their criticality with regard to going live. 80

4. Outsourcing

a. Outsourceability

Fintech institutions may, in principle, outsource functions and activities (principle of outsourceability). The **outsourcing** of essential functions is therefore permitted. The requirements of FINMA Circular 2018/3 "Outsourcing" apply to fintech institutions to an appropriate extent. These requirements must be implemented taking into account the institution's size, complexity, structure, and risk profile. 81

To ensure oversight and control, the outsourced essential functions and the corresponding service providers must be listed in the **OGR**. 82

Companies in supervisory categories 1 through 3 must have a separate risk con-
trol and compliance function serving as independent oversight bodies. For **fintech institutions**, it is sufficient to designate a person on the executive board who is responsible for these functions. Operational risk management and compliance tasks may be outsourced in all supervisory categories. 83

84 **The following may not be outsourced**: senior management, supervision and control by the board of directors, the central management tasks of the executive board, and functions involving strategic decisions. This also applies to decisions regarding the establishment and termination of business relationships.

b. Materiality

85 Determining whether an outsourcing arrangement is material or immaterial may raise questions. Furthermore, outsourcing must be distinguished from collaborations with third-party service providers, which provide services that are not part of the fintech institution's business activities or operational functions vis-à-vis its customers, e.g., direct business relationships with the fintech institution or with the fintech institution's customers. In the latter case, the fintech institution acts not as a contracting party but as an intermediary. **Materiality** is generally affirmed, if the service provider has access to critical data of the supervised entity and could extract or even manipulate this data. Another factor indicating the materiality of an outsourcing arrangement is if a failure on the part of the service provider directly impairs the supervised entity's operational activities. Generally speaking, an increasing number of functions are classified as material due to their direct operational dependence.

86 As a general rule, the following services and functions are presumed to constitute **material outsourcing** in the context of fintech institutions' activities:

- Software and server services that go beyond simple support, provided they directly impact operational activities;
- Core banking system (provided there is a direct, time-critical dependency);
- Cloud-based IT infrastructure;
- SaaS solutions, provided that operations are conducted at the service provider's site and there is thus a direct dependency on operational activities;
- SIC gateway;
- BIN/SIC sponsor (as opposed to card issuers);
- providers of foreign currency transactions, provided that the integration of services goes far beyond the traditional correspondent banking relationship;

- Providers of currency exchange services, provided the process is critical to the fintech institution's operations;
- All control functions/bodies: risk control, compliance function, anti-money laundering unit, internal audit;
- KYC systems (identification and verification when accessing critical data);
- Two-factor authentication;
- Transaction monitoring;
- Role as data protection officer or advisor.

Non-material are generally the following outsourced services and functions: 87

- Verification services (of residential addresses or mobile phone numbers);
- the provision of basic infrastructure (e.g., the Internet) and databases (e.g., sanctions lists for KYC);
- typical staff services (such as legal counsel, business consulting, bookkeeping, financial reporting, tax consulting, human resources, public relations and communications, as well as marketing), as these are easier to replace and, in principle, do not create dependencies.

c. Inventory

Fintech institutions must maintain an up-to-date **inventory** of outsourced 88
functions. This inventory includes a description of the outsourced function, lists the service providers (including subcontractors) and service recipients, as well as the responsible department within the company.

d. Risk Analysis

As part of the outsourcing process, the applicant must prepare a **risk analysis** 89
that covers the key economic and operational considerations as well as the associated risks and opportunities. If multiple functions are outsourced to the same service provider, the concentration risk must be taken into account.

e. Selection, Instruction, and Oversight of the Service Provider

When **selecting** the service provider, its professional qualifications as well as 90
its financial and human resources must be taken into account and reviewed. When deciding on the outsourcing and selecting the service provider, the

possibilities and consequences of a change must also be considered. The service provider must ensure the continuity of service delivery.

91 As part of the **instructions**, the responsibilities of the company and the service provider must be contractually defined and delineated, particularly with regard to interfaces and responsibilities.

92 The outsourced function must be integrated into the company's **ICS**. The material risks associated with the outsourcing must be systematically identified, monitored, quantified, and managed. A responsible unit must be designated within the company to oversee and manage the service provider. The service provider's performance must be continuously monitored and evaluated so that any necessary measures can be initiated in a timely manner.

f. Audit and Supervision

93 The company, its audit firm, and FINMA must be able to verify the service provider's compliance with regulatory requirements. For their benefit, they must be granted, by contract, an unrestricted and unimpeded **right of inspection and audit** at any time with respect to the outsourced function.

94 Audit activities may be delegated to the service provider's auditor, provided that the latter possesses the necessary professional expertise. In the event of such a **delegation**, the company's audit firm may rely on the audit results of the service provider's statutory auditor.

95 The outsourcing of a function must not impede **supervision** by FINMA, particularly in the case of outsourcing abroad.

96 If the service provider is not subject to FINMA's supervision, it must contractually undertake to the applicant to provide FINMA with all **information and documents** regarding the outsourced business area that the applicant requires for its supervisory activities. If audit activities are delegated to the service provider's audit firm, its report must be made available to FINMA, the internal audit department, and the auditing firm of the outsourcing company upon request.

g. Outsourcing Agreements

97 In accordance with the objectives of the outsourcing, the requirements for service provision must be defined and documented prior to the conclusion of

the contract. This includes a **risk analysis** covering the key economic and operational considerations as well as the associated risks and opportunities.

The **responsibilities** of the applicant and the service provider must be contractually defined and delineated, particularly with regard to interfaces and accountability. 98

The applicant must contractually secure the **authority to issue instructions and exercise control** from the service provider. In the case of security-related outsourcing (particularly in the IT sector), the company and the service provider shall contractually define security requirements. Compliance with these requirements must be monitored by the fintech institution. 99

To verify the service provider's compliance with regulatory requirements, the contract must grant a **right of inspection and audit** that is exercisable at any time, is comprehensive, and is unimpeded with respect to the outsourced function. 100

If the (foreign) service provider is not subject to FINMA supervision, it must contractually undertake to the company to provide FINMA with all **information and documents** regarding the outsourced business area that are necessary for supervisory activities. 101

The outsourcing must be based on a **written** contract or a contract in another form that allows for proof through text. In addition to identifying the parties and describing their functions, the contract must contain at least the elements specified in FINMA-RS 2018/3. 102

The institution must ensure that it is informed in a timely manner of the engagement or **change** of subcontractors who perform essential functions. If such subcontractors are engaged, they must be bound by the service provider's obligations and representations necessary to comply with FINMA-RS 2018/3. The possibility of engaging subcontractors must also be regulated in the OGR. 103

In general, contractual provisions must be established to implement the **requirements** of FINMA-RS 2018/3. 104

The institution must define the internal approval procedures for **outsourcing projects** as well as the responsibilities for concluding the corresponding contracts. 105

h. Reporting

106 The implementation of the required supervision and control of the service provider may, in the case of fintech institutions through regular **reporting** by an independent auditor, taking into account the possibility of delegating audit activities to the service provider's auditor. This reporting must enable an assessment of the material risks associated with the outsourcing and the service provider's control activities.

i. Group-related matters

107 With regard to the requirements for the selection, instruction, and control of the service provider, as well as the contractual conditions, the affiliation within the corporate group/**group** may be taken into account, provided that the risks typically associated with the outsourcing demonstrably do not exist or certain requirements are not relevant or are regulated differently.

j. Responsibility and Security

108 The fintech institution remains **responsible** to FINMA as if it were performing the outsourced function itself. It must ensure proper management at all times.

109 For outsourcing arrangements involving security-related functions (particularly in the IT sector), the institution and the service provider shall define contractual **security requirements**. The company must monitor compliance with these requirements.

110 Within this framework, the institution and the service provider shall develop a **security plan** that enables the continued performance of the outsourced function in the event of an emergency. When establishing and implementing the security plan, the company applies the same standard of due diligence as if it were performing the outsourced function itself.

k. Outsourcing Abroad

111 Outsourcing to **abroad** is permitted provided that the institution can expressly guarantee that it, its audit firm, and FINMA can exercise and enforce their rights of inspection and audit. Furthermore, the institution's ability to be re-

structured or wound up in Switzerland must be ensured. Finally, access to the necessary information must be possible at all times in Switzerland.

l. Conditions and Exceptions

In justified cases, FINMA may impose **conditions** on the fintech institution or exempt it, in whole or in part, from compliance with FINMA Guidelines 2018/3. 11 2

Institutions assess and decide on the relevance and implementation of the requirements regarding the selection of the service provider as part of their **risk analysis**. 11 3

Fintech institutions are exempt from the requirement of an orderly reversion with regard to the reversion of the outsourced function. The integration of the outsourced function into the internal control system at fintech institutions may be achieved through regular **reporting** by an independent audit firm. This reporting must enable an assessment of the material risks associated with the outsourcing and the service provider's control activities. 11 4

C. Corporate Governance: Risk Management, Internal Controls, and Compliance (para. 3(b))

1. Basic Principles

Fintech institutions must have an adequately resourced **risk management** system and an **effective internal control system** that ensures, in particular, compliance with statutory and internal corporate regulations (**compliance**) (Art. 1*b*, para. 3, subpara. b, BankG and Art. 14*e*, para. 1, BankV). 11 5

Risk management encompasses the organizational structures as well as the methods and processes used to define risk strategies and risk control measures, and to identify, analyze, assess, manage, monitoring, and reporting of risks. 11 6

The **ICS** comprises the entirety of control structures and processes that, at all levels of the institution, form the basis for achieving business policy objectives and for the proper operation of the institution. The ICS includes not only ex post control activities but also those related to planning and steering. The focus of the ICS is on achieving corporate objectives, protecting corporate as- 11 7

sets, ensuring secure processes, and preventing or detecting irregularities. An effective ICS includes, among other things, control activities integrated into work processes, appropriate risk management and compliance processes, as well as control bodies commensurate with the size, complexity, and risk profile of the institution, in particular an independent risk control and compliance function.

11 8 Examples of potential risks include internal ICT malfunctions, difficulties related to external functions, pandemics, the loss of essential personnel or key clients, liquidity shortages, legal risks, cyberattacks, system failures, supply chain disruptions, widespread or prolonged power outages, natural disasters, data loss, dependencies on third-party service providers, reputational damage, new regulatory requirements, money laundering risks, terrorism, fraud, delays in the payment infrastructure, or currency risks.

119 **Compliance** refers to adherence to legal, regulatory, and internal requirements, as well as observance of industry standards and codes of conduct.

12 0 Fintech institutions must therefore ensure the effective identification, assessment, management, and monitoring of the risks associated with their activities, as well as an effective internal control system (Art. 14*e* para. 1 BankV) . Internal **documentation and guidelines** must specify how these requirements are met (Art. 14*e* para. 2 BankV).

12 1 **Banking secrecy** also applies to governing bodies, employees, agents, or liquidators of fintech institutions (Art. 47 para. 1 lit. a BankG).

12 2 FINMA Guidelines 2017/1 "Corporate Governance—Banks" **do not apply** to fintech institutions, as this would not be constructive given the principle of proportionality set forth therein. With regard to corporate governance, the provisions of the BankG, the Banking Ordinance (BankV), and the CO (as well as the "Swiss Code of Best Practice for Corporate Governance" as a self-regulatory framework) therefore apply. However, FINMA Circular 2017/1 may be consulted as an interpretive aid regarding terminology.

12 3 The **FINMA Circular 2023/01** "Operational Risks and Resilience – Banks," on the other hand, applies directly to fintech institutions, although certain provisions do not apply to them.

2. Independent Control Functions

The units entrusted with the **oversight** of compliance and risk management must be internally independent from profit-oriented business (Art. 14*e* para. 3 BankV). FINMA may grant exemptions from these requirements on a case-by-case basis if the fintech institution: a) generates gross revenue of less than CHF 1.5 million; or b) provides evidence that it has a low-risk business model (Art. 14*e* para. 5 BankV). 12 4

The fintech institution may engage **third parties** to monitor compliance and manage risk, provided that such third parties possess the skills, knowledge, and experience required for this activity, as well as any necessary authorizations. It shall carefully instruct and supervise the engaged third parties (Art. 14*e* para. 4 BankV). 12 5

Fintech institutions generally implement two internal control bodies or **lines of defense**: At the first level, the profit-oriented business units assume responsibility for risk management—in particular through direct monitoring, control, and reporting—and ensure compliance with legal requirements in day-to-day operations (*first line of defense*). At the second level (*second line of defense*), the risk control and compliance functions monitor risks and ensure compliance with legal, regulatory, and internal requirements. Finally, at the third level, an audit may be conducted by Internal Audit (*third line of defense*). Whether and to what extent a fintech institution must ensure these three lines of defense depends largely on the specific circumstances of each case. 12 6

As a rule, only a **second line of defense**—comprising risk control and the compliance function—is required. The units responsible for risk control and compliance must be independent of profit-oriented business activities. Whether the exception provision of Art. 14*e*(4) of the Banking Ordinance (BankV) applies must be assessed on a case-by-case basis. In making this assessment, particular attention must be paid to the risk of conflicts of interest. If conflicts of interest cannot be ruled out, an independent risk management and compliance function must be in place in all cases. Furthermore, the skills and knowledge of the individuals involved, as well as any existing business activities, must be taken into account. 12 7

The BankG and, in particular, Art. 14*e* BankV do not specify internal audit as a (presumably mandatory) component of the ICS for fintech institutions. An **internal audit** is therefore not mandatory for fintech institutions. Whether such 12 8

a function is necessary depends, based on risk considerations, largely on the specific circumstances of each case—that is, on the size and nature of the business activities as well as the existing organizational structure. As a general rule, an internal audit function is not required.3. Risk Management

a. Responsibilities

129 The management of **operational risks** is part of the institution-wide risk management framework. The risk policy and the basic principles of risk management govern the handling of material risks, risk tolerance, and the resulting risk limits across all major risk categories.

130 The **senior management body** approves the framework for managing the operational risks relevant to the institution and monitors compliance with it. At least once a year, it approves the risk tolerance for operational risks in accordance with the risk policy and taking into account the institution's strategic and financial objectives of the institution. In doing so, it takes into account the results of risk and control assessments. It either accepts the extent to which the institution is exposed to operational risks or decides to adjust the risk tolerance and implement the necessary strategic changes, such as a change to the business model.

131 Within this framework, the senior management body regularly approves documented **strategies** for managing ICT, cyber risks, critical data, and BCM, and monitors compliance with them.

132 The **Executive Board** ensures, in a transparent manner, that operational risks are identified, assessed, mitigated, and monitored, and that both the design and implementation of this operational risk management framework are regularly reviewed for effectiveness. To mitigate inherent risks deemed material (so-called "top risks" or "key risks"), it takes supplementary or enhanced risk-specific measures as the situation warrants.

133 If necessary, **FINMA** defines further requirements for operational risk management regarding specific topics as part of its ongoing supervision. This is done in accordance with the principle of proportionality.

b. Inventory

134 Operational risks must be categorized uniformly across the entire institution and recorded in an **inventory**. The categorization may be based on the cate-

gorization of event types used for calculating the minimum capital requirement for operational risks or may be based on an internal taxonomy. The categorization must be applied consistently across all areas of the institution and in all components of operational risk management.

c. Identification

Operational risks include, in particular, ICT risks, cyber risks, risks related to critical data, risks arising from the design and implementation of BCM, and, where applicable, risks arising from cross-border service activities. For a definition, reference may be made to the legal definition in Art. 89 of the Own Funds Ordinance (ERV), according to which operational risks are defined as the risk of losses arising from the inadequacy or failure of internal processes, people, and systems, or from external events. This includes legal risks but excludes strategic risks and reputational risks. 13 5

When **identifying** operational risks, both internal and external factors must be taken into account. The identified operational risks must be assessed in a transparent manner, taking into account both inherent risks and residual risks. Internal factors include, for example, changes in products, activities, processes, and systems, as well as audit findings and internal losses resulting from operational risks. External factors include, for example, identified loss events at other institutions, changes in the security situation (e.g., due to environmental influences, cyberattacks, or terrorism), or changes in regulatory requirements. 13 6

The identification and assessment of operational risks must be based, at a minimum, on the **audit results** and on regularly conducted risk and control assessments. Audit results should (where available) include the findings of the internal audit and the external audit firm, as well as the results of reviews conducted by, for example, the business and organizational units, risk control, the compliance function, or supervisory authorities. 13 7

d. Risk Tolerance

The **risk tolerance** for operational risks takes into account both the tolerance for inherent and residual operational risks and is monitored using risk or control indicators. 13 8

The risk tolerance with respect to **inherent risks** takes into account strategic decisions regarding the business or operating model, e.g., the tolerance for in- 13 9

herent risks associated with serving certain customer segments or countries, offering certain products, using predominantly manual processes, dependence on a complex IT infrastructure, or specific outsourcing arrangements.

e. Employee Training

140 Measures to **raise awareness** among employees to reduce relevant operational risks—in particular ICT risks, cyber risks, risks related to critical data, and risks arising from the design and implementation of BCM—must be implemented, taking into account their tasks, competencies, and responsibilities.

f. Control

141 To assess the existing **control and mitigation measures**, a regular assessment of the effectiveness of key controls must be conducted and documented by an independent audit body (so-called *Design Effectiveness* and *Operating Effectiveness Testing*). Key controls are those control and mitigation measures that minimize the inherent risks deemed material.

142 In addition, the **separation of duties** regarding tasks, competencies, and responsibilities must be reviewed regularly to ensure independence and avoid conflicts of interest. Risk and control assessments must take into account the inherent risks, the effectiveness of existing control and mitigation measures, and residual risks.

143 Prior to **significant changes** to products, activities, processes, and systems, ad hoc risk and control evaluations must be conducted, taking into account the operational risks associated with the change process and the target state. If necessary, the institution must adjust its risk tolerance and implement control and mitigation measures.

g. Reporting

144 **Risk Control** shall report to the senior management body at least annually and to the executive board at least semiannually on operational risks at the highest level of categorization, their comparison with the established risk tolerance, and details of material internal losses.

145 With regard to relevant ICT and cyber risks, the at least annual **reporting** to the Executive Board shall also include information on the development of

these risks, the effectiveness of the corresponding key controls, and significant internal and external events related to these risks.

h. ICT Risks

a. Strategy and Governance

The management of **ICT risks** must take into account the relevant internationally recognized standards and practices, as well as the impact of new technological developments on ICT risks. 146

B Executive managementB ensures that procedures, processes, and controls, as well as roles, authorities, and responsibilities, are implemented and documented for both change management and ICT operations (i.e., *Run*, *Maintenance*). These must be supported by qualified and adequate resources. 147

b. Change Management

For all phases of ICT development or procurement, **change management** must establish procedures, processes, and controls. In each of these phases, it must take into account the impact of the change on ICT risks—in particular, the requirements for confidentiality, integrity, and availability. 148

The Fintech Institute must ensure a **separation** between the development or test environment and the ICT production environment. This also includes a clear assignment of ICT resources and regulations governing the associated access permissions. 149

During the development and procurement of ICT, the functional and non-functional requirements must be clearly defined, approved, and tested and validated according to their **criticality**. 150

c. ICT Operations

As part of its ICT operations, the fintech institution must maintain one or more inventories of ICT components. The **inventory** includes hardware and software components as well as the storage locations of critical data and takes into account both dependencies within the institution and interfaces with key external service providers. The inventory must be readily available and must be regularly reviewed for completeness and accuracy and updated accordingly. 151

15 2 Furthermore, the institution must have procedures, processes, and controls in place that ensure the confidentiality, integrity, and availability of the ICT production environment, taking into account the respective **risk tolerance**.

15 3 Within this framework, the institution must ensure that, in the event of a significant disruption or outage, it can facilitate a seamless transition from ICT operations to its *Business Continuity Plan* (BCP) and *Disaster Recovery Plan* (DCP) processes. To this end, the institution implements appropriate **backup and recovery processes** that are regularly tested and validated.

15 4 Finally, the institution must also implement procedures, processes, and controls that ensure a risk-based approach to ICT when the end of service is imminent or the planned decommissioning date has passed.

d. Incident Management

15 5 The fintech institution has procedures, processes, and controls in place for handling **significant ICT incidents**, including those arising from dependencies on critical external service providers and intra-group outsourcing. In doing so, the entire lifecycle of significant ICT incidents must be taken into account, and roles, authorities, and responsibilities for handling these incidents must be defined.

15 6 The handling of significant ICT incidents must be coordinated with and linked to the **BCM and DRP processes**.

15 7 ICT incidents that the institution classifies as a significant disruption to the performance of its critical processes and that are relevant to supervision must be reported to **FINMA** without delay.

i. Cyber Risks

15 8 The institution must also define clear tasks, competencies, and responsibilities with regard to **cyber risks**. In doing so, it must cover at least the following aspects in accordance with internationally recognized standards and practices, ensuring their effective implementation through appropriate procedures, processes, and controls, and to continuously develop and improve them:

- Identification of the institution-specific **threat potential** posed by cyberattacks and assessment of the possible impacts if vulnerabilities are ex-

ploited with respect to the inventoried ICT components and critical electronic data;

- Protection of the inventoried ICT components and critical electronic data against cyberattacks through the implementation of appropriate **protective measures** (such as data backups, recovery plans, cyber training for employees, participation in bug bounty programs, or source code security reviews), particularly with regard to confidentiality, integrity, and availability;
- Timely recording and detection of cyberattacks based on a process for the systematic and continuous **monitoring** of the inventoried ICT components and critical electronic data;
- **response** to identified vulnerabilities and cyberattacks through the development and implementation of appropriate processes to promptly initiate measures for containment and remediation; and
- ensuring the prompt **recovery** of normal business operations following cyberattacks through appropriate measures.

The applicant must identify the relevant ICS controls related to cybersecurity risks and submit the corresponding supporting documentation (procedures, processes, and controls for detecting, containing, and resolving such a cyberattack) as part of the **cyber risk analysis**. 15 9

Cyber risks are classified as operational risks and should not be equated with ICT risks. Cyber risks are subject to stronger external factors, such as the exploitation of vulnerabilities through various attack vectors—for example, in ransomware or distributed denial-of-service (DDoS) attacks, as well as insider threats. Institutions must therefore include a distinct definition of cyber risks in their risk management framework that does justice to the nature of the risk. 16 0

Cyber risk management must ensure that a successful or partially successful cyberattack is analyzed in terms of its significance for the inventoried critical ICT components, critical electronic data, and critical processes (including outsourced services and functions), and that the **reporting obligation** to FINMA is fulfilled. It is important that the fintech company be immediately informed of any successful or partially successful cyberattacks involving outsourced ICT services and be able to take action, and not merely to fulfill its reporting obligation to FINMA in a timely manner. 16 1

16 2 Following an initial assessment of criticality and an informal preliminary notification to the responsible Key Account Manager at **FINMA** within 24 hours, the report must be submitted in accordance with the requirements catalog of the EHP survey platform (required fields) within 72 hours. Upon completion of the institution's internal case handling, a final root-cause report commensurate with the severity of the incident must be submitted to the responsible department at FINMA. In this context, the applicant must explain how it ensures that the reporting obligation for successful or partially successful cyber incidents of moderate, high, or severe cyber incidents is met.

16 3 The Executive Board regularly commissions **vulnerability analyses** (analyses to identify existing software vulnerabilities and security gaps in the IT infrastructure) **and penetration tests** (targeted testing and exploitation of software vulnerabilities and security gaps in the ICT infrastructure). These must be conducted by qualified personnel with adequate resources. All inventoried ICT components that are accessible via the Internet must be taken into account. In addition, inventoried ICT components that are not accessible via the Internet must be taken into account but which are necessary for the execution of critical processes or contain critical electronic data. The frequency of such analyses and tests must be specified in the relevant documentation.

16 4 Risk- and scenario-based **cyber exercises** must be conducted based on the institution-specific threat potentials. The results of the exercises must be documented and reported in an appropriate form. The scope and content of these exercises are governed by the principle of proportionality. Non-systemically important institutions should conduct at least one annual tabletop exercise—that is, a simulation of a scenario on paper (dry run).

j. Risks to Critical Data

16 5 The fintech institution must establish the basic framework for managing the risks associated with **critical data** relevant to the institution and must monitor compliance with this framework. Critical data refers to data that requires special protection and must therefore be defined by the institution on a risk-based basis. Critical data may be critical in terms of confidentiality, integrity, or availability and are therefore subject to different levels of criticality.

16 6 Critical data with respect to **confidentiality**—i.e., confidential data—is business information or customer or personal data that must be protected from

unauthorized access in order to safeguard the privacy or security of an individual or an organization.

Critical data with respect to **integrity or availability** must be defined by the institution on a risk-based basis. The criticality of this data relates to the institution's ability to operate efficiently and effectively (or at all). Such critical data is therefore vital to the institution's operations. Examples of such "mission-critical data" include data in financial reports (both internal and external), regulatory reports, as well as data used for decision-making, technical implementation, or measuring corporate performance. If this type of data is damaged, destroyed, or becomes inaccessible, the institution and its units and employees may no longer be able to perform their duties. 167

Critical data must be managed throughout its entire **life cycle**. The life cycle encompasses data responsibilities, data collection, storage location, maintenance, retention, deletion, and disposal. It also takes into account aspects of the production, enrichment, processing, and transmission of critical data. 168

169Incidents that significantly compromise the confidentiality, integrity, or availability of critical data must be reported to **FINMA** without delay.

When selecting **service providers** who process critical data (i.e., any handling thereof) or have access to it, due diligence must be given high priority. Clear criteria for assessing how service providers handle critical data must be defined and reviewed prior to entering into a contract. Service providers must be monitored and audited periodically on a risk-based basis as part of the institution's internal control system. 170

k. Business Continuity Management

Each relevant business and organizational unit must identify its critical processes and the resources required for them (particularly with regard to personnel, facilities (e.g., buildings, workplace infrastructure), information, IT systems, or IT infrastructure, etc.) as part of the *Business Impact Analysis* (BIA) and submit this information to FINMA. 171

For its critical processes, the institution must define the *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO) in terms of time frames and submit them to FINMA. These must be coordinated with the necessary service providers. Compliance with the RTO and RPO must be governed by ser- 172

vice level agreements or contracts, or ensured through other appropriate procedures, processes, and controls.

17 3 The institution must define at least one *BCP* and submit it to FINMA; this plan must also describe the circumstances that trigger the plan and the decision-making processes, and take into account the loss of resources. The acceptance of residual risks must be appropriately documented.

17 4 The institution must define at least one *DRP* as part of the BCP. If critical processes or parts thereof are outsourced, the DRP must take into account external dependencies, contractual arrangements, and alternative solutions. The DRP must be reviewed and updated *ad hoc* in the event of significant changes, but at least annually.

17 5 In crisis situations, a **crisis management team** must assume responsibility for crisis management until normal operations are restored. The circumstances triggering a crisis and the tasks, authorities, and responsibilities of the crisis management team must be defined in advance, and the crisis management structure must be aligned with the institution's business activities and geographic structure. The availability of key personnel in the event of a crisis must be ensured. The institution must develop a **communication strategy** for internal and external communication in crisis situations.

17 6 The implementation of the BCP and DRP, as well as the operational effectiveness of the crisis management organization, must be verified through **regular tests**. A systematic plan must be developed for this purpose to ensure regular coverage. Various testing approaches with differing levels of intensity and effectiveness may be selected, such as tabletop exercises.

17 7 The tests must cover various severe but plausible **scenarios** and take into account dependencies during recovery, including dependencies on internal or external third parties. In this context, the technical detection capabilities within the framework of the respective scenario must be demonstrated, for example, by operating a central *Security Information and Event Management* (SIEM) system that provides a unified view of security events across the entire ICT environment, thereby enabling threats to be detected and responded to more efficiently.

17 8 Regular **reporting** to the highest governing body and management provides information on the testing and audit activities carried out and their results. It

highlights the prioritizations made (e.g., prioritization of the critical processes necessary for the performance of critical functions) and the identified gaps in the coverage of other critical processes.

l. Risks Arising from Cross-Border Service Activities

If institutions or their group companies **provide cross-border services** or distribute financial products across borders, the risks arising from the application of foreign legal provisions (tax, criminal, and anti-money laundering laws, etc.) must also be appropriately identified, mitigated, and monitored. The corresponding risk analysis must be submitted to FINMA. To ensure compliance with foreign legal provisions, the institutions must submit corresponding country manuals to FINMA. 17 9

Institutions shall subject their cross-border service business and the cross-border distribution of financial products to an in-depth analysis of the legal framework and the associated risks. Based on this analysis, the institutions shall take the necessary strategic and organizational **measures** to eliminate and minimize the risks and continuously adapt these measures to changing conditions. In particular, they must possess the necessary country-specific expertise, define country-specific service models, train employees, and ensure compliance with the requirements through appropriate organizational measures, guidelines, compensation models, and sanction models. The corresponding cross-border guideline must be submitted to FINMA. 18 0

Risks arising from external asset managers, intermediaries, and other service providers must also be taken into account. Due care must be exercised in the **selection and instruction** of these partners. 18 1

This principle also applies to situations in which a **subsidiary, branch, or similar entity of a Swiss institution domiciled abroad** provides cross-border client services. 18 2

m. Operational Resilience

The institution identifies its critical functions (strategically most important operations or service provision) and their tolerance levels for disruption. These are approved by the senior management body. In addition, the senior management body regularly approves and monitors the procedures for ensuring **operational resilience**. This refers to the ability to withstand significant opera- 18 3

tional shocks with the least possible negative impact and to overcome them in a timely manner.

18 4 As part of the operational resilience assessment, the applicant must define **critical functions** and specify a higher tolerance for disruption (e.g., 1–5 days) for each critical function. The critical functions must be distinguished from the BCM, and an overarching *Tolerance for Disruption* must be defined.

18 5 On this basis, the institution must establish appropriate **measures** to ensure operational resilience, taking into account severe but plausible scenarios. The approach should be preventive in nature, incorporating targeted precautionary measures, the development of the operating model, and continuous learning and improvements to make the critical functions as resilient as possible ("Resilience by Design").

4. Anti-Money Laundering Unit

18 6 Fintech institutions are subject to the AMLA (Art. 2(2)(a) AMLA). The **anti-money laundering due diligence obligations** are governed by Title 5 of the GwV-FINMA (Art. 3(1) in conjunction with Art. 43*a* AMLO-FINMA). In addition, FINMA Circular 2016/7 "Video and Online Identification" applies to fintech institutions.

18 7 Fintech institutions must, among other things, prepare a **money laundering risk analysis** that encompasses various elements: The analysis must first define the risk tolerance by explicitly excluding certain risks. Furthermore, the analysis must specify how and which money laundering risks are taken into account. Finally, the fintech institution must define key performance indicators and thresholds to demonstrate compliance with its own business strategy and risk policy, as well as their evolution over the years. Thus, the risk analysis contains the essential information regarding the intended approach to managing money laundering risks.

18 8 **In terms of content**, the structure of the money laundering risk analysis depends heavily on the fintech institution's actual operational and geographic business activities. The following may serve as useful risk categories in some cases: a. Customer structure (country risks, customer segments, closeness of the relationship with the customer), b. Type of customer relationship/complex structures, c. Business activities (products and services), d. Business relation-

ships with heightened risks (PEPs, shell companies), e. Transaction-related risks and the like.

Financial intermediaries must have an **appropriate function** in place to combat money laundering and terrorist financing (including sanctions evasion). The individuals entrusted with these tasks must be appropriately trained and have the necessary resources to perform their duties appropriately. The relevant internal regulations must be documented in an appropriate form and made available to the employees entrusted with these tasks. In doing so, the applicable legal provisions must be implemented internally. 189

Fintech institutions may benefit from **organizational simplifications** regarding the anti-money laundering unit, provided that the institution also meets the requirements for simplifications in the area of compliance/risk management (Art. 14*e* para. 5 BankV) and the objective of combating money laundering and terrorist financing is not precluded by the simplifications (see Art. 75*a* GwV-FINMA). Depending on the money laundering risk, FINMA may grant further exemptions or impose stricter requirements (see Art. 3 para. 2 GwV-FINMA). 190

5. Documentation and Processes

As a rule, applicants must submit guidelines (Board of Directors' regulations or Executive Management directives) as **documentation**: 191

- general organization and responsibilities regarding risk management (often described in the Organizational and Governance Regulations [OGR]);
- business strategy and risk policy;
- risk analysis;
- general risk management;
- general control matrix (including responsibilities, frequencies, and control activities) ;
- Operational risks (including ICT/cyber risks, risks related to critical data and data protection/security, and Business Continuity Management [BCM]);
- Compliance in general;
- Money laundering and sanctions in particular;

- if conducting business abroad: cross-border operations, including country manuals;
- Outsourcing (and corresponding outsourcing agreements) ;
- Safekeeping of public deposits and monitoring of the CHF 100 million threshold;
- Employee conduct;
- Handling of dormant assets (see Art. 37*l* and Art. 37*m* of the BankG, as well as Art. 45 et seq. of the Banking Ordinance);
- where the FIDLEG applies: Conduct toward customers.

6. Avoidance of Conflicts of Interest

19 2 Fintech institutions must take appropriate organizational measures to avoid **conflicts of interest** that may arise in the provision of their services or to prevent clients from being disadvantaged by conflicts of interest. If a conflict of interest cannot be ruled out, this must be disclosed (Art. 14*g* BankV), and clients must be informed accordingly. The self-interests of the licensee and its employees must not conflict with the interests of clients. Likewise, the interests of clients must not conflict with one another.

D. Financial Requirements (para. 3(c))

1. Business Plan

19 3 The applicant must submit a **business plan**, including a budget (balance sheet, income statement), for the next three fiscal years, covering optimistic, realistic, and pessimistic scenarios. Liquidity planning for the first fiscal year must be based on the pessimistic scenario outlined in the business plan (on a monthly basis).

19 4 Fintech institutions must have a **business model** that ensures independent and ongoing compliance with their financial obligations. Setting the licensing threshold too low and having an excessively high risk appetite must be prevented. If, for structural reasons, an institution cannot generate a profit and can only survive with the help of grants from its stakeholders (non-repayable) can survive, this constitutes a deficiency that calls into question its eligibility for authorization. In such cases, the institute's continued existence depends

solely on the solvency and willingness of the beneficial owners, which constitutes an unacceptable risk from both creditor protection and operational stability perspectives. Even a surplus of equity and the determination of the beneficial owners to cover the operating losses incurred year after year—so that there is no immediate danger to creditors—do not, under these circumstances, , do not justify a state of persistent insufficient profitability. To demonstrate that the applicant can meet these requirements, it must, in particular, present the aforementioned realistic and well-founded economic scenarios.

In this sense, FINMA's **supervision** does not guarantee the commercial success of the supervised institutions, but rather serves to protect customers. As part of the licensing process, FINMA verifies that the business plans and financing plans are plausible. Such an examination is all the more important given that customers of entities under Art. 1*b* of BankG are not protected in the event of the entity's bankruptcy (namely, their claims are subordinate to wage claims) and that bankruptcies in this sector are not uncommon and can even occur in the early stages. 19 5

In the corresponding **analysis** of the business model, the following points, among others, must be taken into account: 19 6

- Identification of the key risks of the business model;
- Assessment of the institution's ability to adapt to any changes in circumstances;
- Analysis of the available financial resources and other resources for implementing the strategy;
- Evaluation of the institution's strategy and risk appetite;
- Consideration of the market and business environment and comparison of the company's growth ambitions with those of other providers;
- Assessment of the feasibility or plausibility of the business plan's assumptions;
- Review of the institution's profitability to ensure a sufficient return on capital and the continuity of its business operations (including adequate coverage of financing costs [debt and equity] and operating expenses).

19 7 If the fintech institution under review is part of a **group**, the above criteria must be assessed not only at the level of the individual institution but also at the group level.

2. Liquidity

19 8 Fintech institutions must have adequate **financial resources** (Art. 1*b*, para. 3, let. c, BankG). The scope of business and its geographic reach must be commensurate with the fintech institution's financial capabilities (Art. 14*b*, para. 2, Banking Ordinance).

19 9 For risk management purposes, FINMA requires that a fintech institution have sufficient liquid funds at the time of authorization to cover at least its fixed costs during the initial phase, taking into account any potential income. To this end, the fintech institution must submit an up-to-date, detailed **liquidity plan** (on a monthly basis) and, as a prerequisite for authorization, provide evidence (bank statements, etc.) of its current liquidity position.

20 0 To ensure solvency, the fintech institution must incorporate **liquidity risks** into its risk management framework and monitor them on an ongoing basis as part of its internal control system.

3. Minimum Capital

20 1 To obtain a license, a fintech institution must demonstrate that it has fully paid in the minimum capital specified by the Federal Council (Art. 1*b*, para. 1, in conjunction with Art. 3, para. 2, letter b, of the BankG). Fintech institutions must have **minimum capital** amounting to 3 percent of the public deposits received and the crypto-based assets held in collective custody, but at least CHF 300,000. It must be fully paid up and maintained at all times.

20 2 The minimum capital must be used for the **purpose** of the company. It may therefore not be lent to qualifying shareholders or to natural or legal persons closely associated with them, nor may it be invested in equity interests controlled by them (Art. 17*a*(1) Banking Ordinance). This restriction on investment options is intended to reduce the risk of the company being stripped of its assets (fraud risk). The provisions of the ERV and the LiqV do not apply in the absence of maturity transformation (Art. 17*a* para. 3 BankV).

20 3 Nevertheless, certain **liquidity and counterparty risks** exist. Therefore, even in the case of persons under Art. 1*b* BankG, it must be ensured that they

have sufficient financial resources to bear their risks. The minimum capital is intended not only to provide a certain level of protection for deposits but, above all, to ensure that the institution has adequate organizational and technical resources.

FINMA may set **higher capital requirements** in individual cases if this appears necessary due to the risks associated with the business (Art. 17*a* para. 2 BankV) . The calibration of capital requirements is intended to ensure fair and equal application across different business models. The additional capital pursuant to Art. 17*a*(2) of the Banking Ordinance (BankV) is intended to enable authorized institutions to remain viable for a minimum period. 20 4

To **demonstrate** compliance with the financial requirements, the applicant must submit the following information: 20 5

- appropriate evidence of compliance with the minimum capital requirements and a description of how compliance with the minimum requirements will be ensured as public deposits increase;
- projected development of minimum capital based on the business plan, including details on sources of financing.

E. Guarantee (para. 3(d))

Persons entrusted with executive functions—at the three levels of qualified shareholders, executive management, and the board of directors—must be of good repute and provide **a guarantee of sound business conduct** (Art. 1*b*, para. 3(d) of the BankG) (so-called "guarantee persons") . The assessment of suitability encompasses two components: professional competence ("fitness") for the specific role, as well as the personal integrity ("properness") of these individuals. To assess suitability and good reputation, information and documents are requested along with the application regarding the persons of good repute (see Art. 8 Banking Ordinance). 20 6

To demonstrate compliance with the requirements for members of the body entrusted with management and for executive management, the following **documents** must be submitted: 20 7

- Personal information;
- A copy of a valid identification document (signed and dated copy of a passport or ID card);

- A copy of the residence or settlement permit for foreign nationals (signed and dated copy);
- criminal record extract (not older than 3 months);
- criminal record extract from the previous country of residence and/or country of origin for foreign nationals who have resided in Switzerland for less than 5 years (not older than 3 months);
- debt collection register extract or equivalent confirmation (not older than 3 months);
- Curriculum vitae signed by the person concerned (including details of education and professional training and at least two references); Record and description of past and current professional activities and mandates, including years and dates);
- Contract with the applicant (signed and dated);
- Declaration regarding pending and concluded proceedings (Form B1, signed and dated);
- Declaration regarding qualifying holdings (Form B3, signed and dated);
- Declaration regarding other mandates (Form B3, signed and dated).

20 To this end, FINMA requires the applicant (using the **forms** specified by FIN-
8 MA for this purpose) to submit the following information **regarding holdings, i.e., the shareholder structure:**

- Share capital (structure, allocation, par value, payment, etc.);
- A list of all shareholders with a direct or indirect stake of 5 percent or more (traced back to the beneficial owner, specifying voting rights and capital stake);
- a diagram showing all direct or indirect qualified shareholders down to the beneficial owners (including the size of each holding), broken down by voting rights and capital shares;
- information on any agreements as well as other means of control or significant influence; Documents such as shareholder agreements or investment agreements must be submitted;
- Declaration regarding holders of qualifying interests (Form A1; to be submitted by the applicant);

- Supplementary sheet to the declaration regarding holders of qualifying interests (Form A2; one per qualifying stakeholder; to be submitted by the applicant).

Qualified shareholders must also be of good repute and ensure that their influence does not adversely affect prudent and sound business operations. However, they need not be independent of management. A qualified shareholder is defined as anyone who holds at least **10 percent** of the voting rights or capital, or who can otherwise significantly influence business operations (Art. 14*d* para. 3 BankV). The phrase "in any other way" serves not only to clarify the purpose of the provision but also has independent significance. It is intended to capture additional factual and legal influences regardless of threshold values. 209

For holdings exceeding **5 percent**, the evidence listed in the FINMA Guidelines. 210

Documentation required for natural persons acting as direct or indirect **qualified participants** includes: 211

- Personal information;
- A copy of a valid identification document (a copy of a passport or ID card signed and dated by the holder);
- criminal record extract (not older than 3 months);
- criminal record extract from the previous country of residence and/or country of origin for foreign nationals who have resided in Switzerland for less than 5 years (not older than 3 months);
- debt collection register extract or equivalent confirmation (not older than 3 months);
- A resume signed by the person in question (including details of education and professional training, at least two references, and a record and description of past and current professional activities and mandates, including years and dates);
- A declaration stating whether the qualifying interest is held for the person's own account or in a fiduciary capacity for third parties, and whether the qualifying person has granted options or similar rights in connection with

this interest (Forms: Declaration by Direct/Indirect Qualified Shareholders, signed and dated);

- Declaration regarding pending and concluded proceedings (Form B1, signed and dated);
- Declaration regarding Qualified Shareholdings (Form B2, signed and dated).

21 2 The required documentation for **legal entities** acting as direct or indirect qualified shareholders includes:

- a detailed description of the organization, business activities, financial situation (including the most recent annual financial statements, if available), and, if applicable, the group structure;
- an extract from the debt collection register or equivalent confirmation (not older than 3 months);
- an extract from the commercial register or a corresponding confirmation;
- a declaration stating whether the qualifying interest is held for the holder's own account or in a fiduciary capacity for third parties, and whether the qualifying party has granted options or similar rights with respect to this interest (Forms A3/A4, signed and dated);
- Declaration regarding pending and concluded proceedings (Form B1, signed and dated);
- Declaration regarding qualifying holdings (Form B2, signed and dated).

F. Financial Reporting and Auditing (para. 4, lit. a, b, and c)

21 3 **Accounting** and the audit of the annual financial statements are governed exclusively by the provisions of the CO (Art. 1*b*, para. 4, subpar. a, BankG), and a limited audit cannot be waived (no opting-out pursuant to Art. 727*a*, paras. 2–5, CO) (Art. 1*b*, para. 4, subpar. b, BankG) . If public deposits are not segregated from equity, a full audit must be conducted (Art. 14*f*, para. 1, subparagraph b of the Banking Ordinance). Ideally, the institution conducts a full audit in accordance with Art. 727 of the CO.

21 4 Fintech institutions must engage a licensed **auditing firm** to perform the regulatory audit pursuant to Art. 24 of FINMASA (Art. 1*b*, para. 4, subpara. c, BankG). For this purpose, they must designate an audit firm licensed under

Art. 9a AOA (see Art. 24 para. 1 lit. a FINMASA). The application for authorization must be accompanied by a declaration of acceptance from the regulatory audit firm as well as a completed questionnaire regarding the services of licensed audit firms, which can be found on FINMASA's website.

G. Disclosure Requirements (para. 4, letter d)

The provisions on privileged deposits and immediate payment (Art. 37*a* and Art. 37*b* of the BankG) (deposit insurance) are **not applicable** to public deposits and crypto-based assets accepted by a fintech institution. Before accepting deposits, depositors must be informed of the **lack of deposit insurance and** the **lack of bankruptcy protection**, and must be advised of the possible consequences (Art. 1*b*, para. 4, letter d, BankG) . 215

Pursuant to Art. 7*a* para. 1 of the Banking Ordinance (BankV), customers must be informed in writing or in another **verifiable text-based form** (in a separate document, within the business model documentation, or separately via email) about the lack of deposit insurance, as well as about the fintech institution's business model, its services, and the risks associated with the technologies used. 216

Customers must be informed in such a way that they have sufficient time **before entering into the contract** to understand the information in light of the contract (Art. 7*a*(2) BankV). Merely providing information through general terms and conditions is not sufficient (Art. 7*a*(3) BankV). 217

If the information is made available **electronically**, the persons referred to in Art. 1*b* of BankG must ensure that it can be accessed, downloaded, and recorded on a durable medium at any time in all relevant (official) languages of the target customers (Art. 7*a*, para. 4, BankV). A durable medium is defined as paper or any other medium that enables the storage and unaltered reproduction of information (Art. 7*a*, para. 5, BankV). 218

The applicant must submit to FINMA details regarding the information provided to customers in accordance with Art. 7*a* of the Banking Ordinance (BankV). To this end, the relevant text as well as the corresponding **onboarding process**, including screenshots of the individual steps, must generally be submitted. The information regarding risks related to the business model, services, and technologies used must be detailed. The notice regarding the non-application of the provisions on privileged deposits (Art. 37*a* BankG), immedi- 219

ate payout (Art. 37*b* BankG), and deposit insurance (Art. 37*h* et seq. BankG) must be complete and clearly highlighted. Procedurally, the information must be structured such that, if consent is not given, the customer onboarding process is terminated. A mere reference to Art. 7*a* BankV is in any case insufficient. Customers must actively consent to the information (e.g., by checking a box with a mouse click).

V. SPECIAL CASES (INCLUDING PARAS. 5 AND 6)

A. Possible Increase in the Threshold for Public Deposits by FINMA (paras. 5 and 6)

220 If public deposits exceed the threshold of CHF 100 million, this must be reported to FINMA within 10 days, and a **banking license application** pursuant to Art. 1*a* of the BankG must be submitted within 90 days (subject to para. 5) (Art. 1*b* para. 6 of the BankG) . There appears to be no need for this transitional provision, since a person under Art. 1*b* of the BankG is already supervised by FINMA and maintains regular communication with it, such that approaching the threshold of CHF 100 million can readily be addressed in a timely manner in this context.

221 The Federal Council may adjust the amount of **CHF 100 million**, taking into account the competitiveness and innovative capacity of the Swiss financial center (Art. 1*b* para. 2 of the BankG). In justified individual cases, FINMA also has the option to waive the CHF 100 million cap: In special cases, it may declare paragraphs 1–4 applicable to persons who, on a commercial basis, accept public deposits exceeding CHF 100 million or publicly commit to neither investing nor paying interest on such deposits and to ensuring customer protection through special measures (Art. 1*b* para. 5 BankG).

B. Combination with Other Licensing Categories

222 Combining the activities of a fintech institution with those of a **securities firm** is not generally precluded. The same applies to activities as an **asset manager**, although various regulatory coordination issues arise:

- in particular, it should be noted that the fintech license falls outside the **licensing cascade** (see Art. 6 FinIA);

- when combining license categories, the higher **capital adequacy requirements** of the two license categories apply;
- finally, when combining a fintech license with a securities firm license, the operational challenge lies in the different treatment of deposits: while there is no deposit insurance for fintech institutions (Art. 1*b* para. 4 lit. d BankG), customers of securities firms that maintain settlement accounts benefit from **deposit insurance**, which requires a separation of the respective cash accounts. For entities under Art. 1*b* of BankG, it would therefore likely be more effective to conduct any customer trading activities through a separate legal entity.

C. Consolidated Supervision

The provisions of the Banking Act (BankG) on consolidated supervision apply mutatis mutandis to persons under Art. 1*b* BankG, subject to special provisions under Art. 1*b* para. 1 BankG. This also applies to the banking consolidation law set forth in Art. 3*b* et seq. BankG and Art. 21 et seq. BankV. If an entity under Art. 1*b* BankG is part of a financial group, authorization may be made contingent upon appropriate **consolidated supervision** by a financial market supervisory authority (Art. 1*b* para. 1 in conjunction with Art. 3*b* BankG). 22 3

The **FINMA Circular 2025/4** "Consolidated Supervision of Financial Groups under the BankG and FinIA" sets forth the supervisory authority's practice regarding subjection to consolidated supervision, as well as its scope and content. By analogy, the circular also applies to financial groups controlled by persons under Art. 1*b* of the BankG and to persons under Art. 1*b* of the BankG who are part of a financial group (Art. 1*b*(1) in conjunction with Art. 3*c*(1) of the BankG) . 22 4

Accordingly, FINMA may require consolidated group supervision in cases involving **group-related matters**. If other foreign authorities simultaneously claim full or partial supervision over the financial group, FINMA shall, while preserving its own powers, consult with those authorities regarding the respective jurisdictions, modalities, and scope of group supervision. Before making its decision, FINMA shall hear the companies of the financial group incorporated in Switzerland (Art. 3*d* para. 2 BankG). 22 5

For this purpose, a **financial group** is defined as two or more companies if: a) at least one company operates as an entity under Art. 1*b* BankG or holds a fin- 22 6

tech license; b) they are primarily active in the financial sector; and c) they form an economic unit *or*, based on other circumstances, it can be assumed that one or more of the companies subject to individual supervision are legally obligated or de facto compelled to assist group companies (Art. 1*b*(1) in conjunction with Art. 3*c*(1) of the BankG).

22 7 A legal or de facto **obligation to provide support** pursuant to Art. 21 para. 2 of the Banking Ordinance (BankV) may arise, in particular, from the following circumstances:

- strategic, personnel, organizational, or financial interdependencies;
- cooperations and dependencies;
- the use of a common business name;
- a uniform market presence; or
- letters of comfort, keep-well agreements, or similar safeguards.

22 8 The circumstances listed by name are not exhaustive. Thus, other connections may also trigger a de facto obligation to provide support if they could give third parties the impression of an **integrated system**. The higher the ownership stake, the less significant the other connecting elements need to be to justify inclusion in consolidated supervision in the overall assessment.

22 9 According to para. 4(1) of the Banking Ordinance (BankV), a person is active in the **financial sector** if they: a) provide or broker services for financial transactions, in particular, conducts deposit or credit business, securities trading, investment business, or asset management for itself or for third parties, or accepts crypto-based assets pursuant to Art. 5*a* of the Banking Ordinance; b) holds qualifying interests predominantly in companies operating in the financial sector (holding company); or c) is a significant group company as defined in Art. 3*a* of the Banking Ordinance.

23 0 The **activities** specifically listed in Art. 4(1)(a) of the Banking Ordinance are not exhaustive. Consequently, other business activities may also constitute activities in the financial sector. These include, in particular, finance leases, factoring, credit card business, participation in securities issues, as well as the custody of securities, payment services, and the issuance and custody of means of payment (including payment tokens). For the purposes of consolidated supervision, group companies that engage in purely commercial, indus-

trial, or administrative activities are considered not to be active in the financial sector.

Companies form an **economic unit** if one of the companies holds, directly or indirectly, more than half of the voting rights or capital in the other companies, or otherwise controls them (Art. 21 para. 1 BankV). According to Art. 21 para. 2 BankV, an obligation to provide support may arise, in particular, due to: a) personnel or financial interdependencies; b) the use of a common corporate name; c) a unified market presence; or d) letters of comfort. Group companies are companies linked by an economic unit or an obligation to provide support (Art. 22 BankV). 23 1

The inclusion of a company in consolidated supervision may also be triggered without a majority stake ("controlled in some other way"), provided that other legal or factual elements indicate the existence of an affiliated system. Such elements include, in particular, personnel, organizational, financial, or business-related **interconnections and dependencies**. If a person is controlled under Art. 1*b* of the BankG by one or more natural persons who control other companies supervised by FINMA or other significant companies operating in the financial sector, a so-called *de facto* financial group may exist, which must be subject to consolidated supervision. 23 2

FINMA may subject a financial group to **group supervision** if it: a) operates in Switzerland an entity organized under Swiss law pursuant to Art. 1*b* of BankG; or b) is effectively managed from Switzerland (Art. 1*b*, para. 1, in conjunction with Art. 3*d*, para. 1, BankG). Group supervision by FINMA covers all group companies of a financial group that are active in the financial sector (Art. 23, para. 1, BankG). 23 3

In justified cases, FINMA may **exclude** financial group companies from consolidated supervision or declare its provisions to be only partially applicable to them, particularly if a group company is immaterial for the purposes of consolidated supervision (Art. 23 para. 2 Banking Ordinance) . FINMA may **include**, in whole or in part, a financial sector entity that is controlled jointly by a financial group supervised by FINMA and third parties within the scope of consolidated supervision (Art. 23 para. 3 of the Banking Ordinance). 23 4

Based on considerations of investor and creditor protection, FINMA applies the **principle of consolidated supervision** to group structures involving 23 5

fintech institutions, while taking into account the specific risks of each individual case.

23 6 The definition of the **scope of consolidation** for FINMA's consolidated supervision is determined in consultation with the competent foreign supervisory authority in accordance with Art. 3*d* para. 2 of the BankG and includes, in particular, determining which authority is the primary supervisory authority (*lead regulator*). Furthermore, it is inherent in consolidated supervision that all relevant supervisory authorities coordinate with one another regarding their respective responsibilities and the modalities of cooperation. The modalities of supervisory cooperation and information exchange are established on a case-by-case basis or generally between supervisory authorities. This ensures that neither gaps nor duplications arise.

23 7 To address group-wide risks, FINMA may, in accordance with the principle of proportionality, instead of consolidated supervision or a denial of authorization, order appropriate, preventive structural measures for **ring fencing** (*ring fencing*) or other measures (e.g., adjustment of the group structure).

23 8 In the case of foreign control, however, the consent of the relevant **foreign supervisory authorities** must be obtained in any event (see Art. 1*b*(1) in conjunction with Art. $3^{bis}(1^{bis})$ of the BankG). Consolidated supervision should, in principle, cover all supervisory areas (qualitative and quantitative consolidation).

23 9 In the case of group activities, the applicant must:

- submit an **organizational chart** of the group, including information on existing or planned financial market licenses, a graphical representation, and the voting rights and capital shares; as well as
- a detailed description of all strategic, personnel, organizational, or financial **links** between the applicant and all group companies.

D. Cross-Border Matters

24 0 Fintech institutions may operate abroad, be under foreign control, and/or belong to a foreign financial group. In addition, the question arises of reciprocity and the recognition of foreign licensing categories as equivalent to the fintech license, and thus the question of whether branches and representative offices are possible.

1. Foreign Business (*outbound*)

Fintech institutions may conduct active or even merely passive **foreign business** in the sense of cross-border service provision. Any foreign business conducted by fintech institutions leads to an increase in the risks associated with business operations and to an expansion of the compliance scope. Accordingly, the risks arising from the application of foreign legal provisions (tax, criminal, anti-money laundering laws, etc.) must be appropriately identified, classified, and mitigated through a risk analysis (strategic and organizational measures, expertise, country-specific service models, training, and partner selection) and controlled (through guidelines, compensation models, and sanction models) . 24 1

Due to foreign law, **active international business** generally requires the fintech institution to have some form of local administrative organization abroad. Accordingly, fintech institutions organized under Swiss law must file a notification with FINMA before establishing a subsidiary, branch, agency, or representative office abroad (Art. 1*b*, para. 1, in conjunction with Art. 3, para. 7, BankG). The notification that a fintech institution must submit to FINMA before commencing operations abroad must contain all information and documents necessary for assessing the business activities, namely: a) a business plan that describes, in particular, the nature of the planned business activities and the organizational structure, b) the address of the foreign branch, c) the names of the persons entrusted with administration and management, d) the auditing firm, e) the supervisory authority in the host country (para. 20 Banking Ordinance) . The fintech institution must also report the cessation or any material change in its business activities abroad, as well as any change in the auditing firm or the supervisory authority (Art. 20 para. 2 BankV). 24 2

Even in the case of purely **passive foreign business**, this must be described in the OGR in terms of a precise factual and geographical definition of the scope of business (see Art. 1*b*(3)(a) of the BankG; Art. 14*b*(1) of the Banking Ordinance). This results in heightened requirements for internal administrative organization and corporate governance. Accordingly, the organization and documentation of risk management and compliance must address the relevant risks and controls. This generally includes, in particular, a cross-border policy, including so-called country manuals for the countries in question. If fintech institutions that have already been authorized wish to commence new passive foreign business, this constitutes a material change to the basis for authoriza- 24 3

tion and therefore requires prior approval (see Art. 8*a* para. 2 of the Banking Ordinance). It is not possible to commence such activities in the OGR on a provisional basis.

2. Foreign Control

24 4 FINMA may make the authorization to establish a fintech institution—which is to be organized under Swiss law but over which there is, for example, a **controlling foreign influence** (see Art. 3bis para. 3 of the BankG) through shareholders or group companies domiciled abroad—subject to the following additional conditions (Art. 1*b* para. 1 in conjunction with Art. 3bis para. 1 of the BankG):

1. the guarantee of **reciprocity** by the states in which the foreign parties holding qualifying interests are domiciled or have their registered office (see Art. 19 para. 1 of the Banking Ordinance (BankV)), provided that no international obligations to the contrary preclude this (see Art. 3^{quater} of the BankG); and

2. the use of a **company name** that does not indicate or suggest that the fintech institution is of Swiss character.

24 5 The same applies to fintech institutions that are foreign-controlled after their incorporation or if the foreign parties holding qualifying interests change (Art. 1*b*, para. 1, in conjunction with Art. 3ter, paras. 1–2, BankG) . Applications for such **additional licenses** as a foreign-controlled fintech institution must contain the information specified in Art. 8 of the Banking Ordinance (BankV) (Art. 18 BankV).

3. Representative Offices (*inbound*)

24 6 Pursuant to the general reference by analogy in Art. 1*b* para. 1 of the BankG, the provisions of the BankG apply mutatis mutandis to branches established or representatives appointed in Switzerland by "foreign persons as defined in Art. 1*b* of the BankG" (Art. 1*b* para. 1 in conjunction with Art. 2 para. 1 of the BankG). Pursuant to Art. 2 para. 1 of the BankG, the FINMA Foreign Banks Ordinance (ABV-FINMA) also applies mutatis mutandis to fintech institutions.

24 7 Accordingly, a "**foreign entity** under Art. 1*b* of the BankG" is defined as any company organized under foreign law that holds a license abroad recognized as equivalent to a fintech license or that carries out the activities of a "person

under Art. 1*b* of the BankG" (Art. 1*b*(1) in conjunction with Art. 2 of the BankG in conjunction with Art. 1(1) of the ABV-FINMA).

A "foreign entity under Art. 1*b* BankG" requires a **license** from FINMA if it employs persons in Switzerland who, on its behalf, conduct business in Switzerland or from Switzerland on a permanent and commercial basis, maintain customer accounts, or enter into legal obligations on its behalf (so-called branch office), or if it otherwise acts on behalf of "foreign entity under Art. 1*b* of the BankG," namely by forwarding client orders to it or representing it for promotional or other purposes (so-called "representation") (Art. 1*b*(1) in conjunction with Art. 2 of the BankG in conjunction with Art. 2(1) of the FINMA Ordinance). 248

The ABV-FINMA does not apply if the "foreign entity pursuant to Art. 1*b* of the BankG" is in fact managed from Switzerland or conducts its business exclusively or predominantly in or from Switzerland, since in such cases the **ordinary licensing requirements** of the BankG apply (see para. 1(2) of the ABV-FINMA). 249

Art. 19 para. 2 of the Banking Ordinance (BankV) specifies that, when establishing a permanent **representative office** of a "foreign entity pursuant to Art. 1*b* of the Banking Act (BankG)," reciprocity is also guaranteed if Swiss banks are permitted to open permanent representative offices with the same functions in the foreign country. Art. 19 para. 2 of the Banking Ordinance (BankV) thus does not require that Swiss financial intermediaries also be able to open representative offices abroad. Furthermore, the Federal Council is authorized, on the basis of the mutual recognition of equivalent supervisory regulations and measures, to conclude international treaties that provide that "foreign persons under Art. 1*b* of the BankG" from the contracting states may open a branch or a representative office without authorization from FINMA (Art. 1*b*, para. 1, in conjunction with Art. 2, para. 3, of the BankG). Conversely, FINMA may subject "foreign persons under Art. 1*b* of the BankG" in full to the provisions applicable to domestic fintech institutions, provided that the law at the place of business of the "foreign persons under Art. 1*b* of the BankG" does not grant Swiss fintech institutions equivalent exemptions and no international treaty precludes this (see Art. 3 para. 2 of the FINMA Ordinance). 250

As a first step, the question arises as to which foreign legal forms meet the requirements for a fintech license. If such **equivalence**—and thus the require- 251

ment for authorization—is affirmed, the next question is whether both a branch and a representative office are eligible for authorization under the analogous application of the ABV-FINMA.

VI. CHANGES TO AUTHORIZATION

25 2 Fintech institutions must report any **change** in the facts underlying the authorization (Art. 8*a*(1) BankV) to FINMA. If the changes are material, prior authorization from FINMA must be obtained to continue operations (para. 8*a*(2) BankV). Significant substantive changes to the business model during the term of the supervisory relationship (e.g., a change in the business model) may necessitate an amendment to the Articles of Association and, if applicable, to the bylaws.

25 3 No. II of the **FINMA Guidelines** on Fintech Licensing provides a non-exhaustive list of what qualifies as a material change within the meaning of Art. 8*a*(2) BankV and therefore requires prior approval from FINMA. This includes the following changes:

- Changes to organizational documents (in particular the articles of association and the OGR; see also Art. 10(a) of the Financial Institutions Ordinance (FINIV);
- changes concerning qualified participants (see Art. 10(d) and (e) FINIV for further details);
- changes in the persons entrusted with administration or management (see also Art. 10(b) FINIV);
- Changes regarding the organization (e.g., changes to risk control or the compliance function);
- if applicable: Changes to the technical setup regarding the custody of crypto-based assets;
- Changes regarding internal corporate governance regulations;
- Changes regarding business activities and ancillary services (business area);
- Changes regarding the outsourcing of essential services;
- The commencement, modification, or discontinuation of foreign business operations (subsidiaries, branches, and representative offices must always be listed in the OGR as well);

- Mergers, demergers, conversions, or transfers of assets pursuant to the Merger Act of October 3, 2003 (FusG); and
- Change of audit firm in Switzerland and abroad.

The **application** for approval of the change must include a detailed justification (including a risk analysis). All relevant information must be documented, and the amended documents must also be submitted in a version highlighting the changes. Depending on the nature of the changes, it is recommended to discuss them with FINMA in advance. 25 4

VII. APPROVAL HISTORY

To date, FINMA has approved a **total of 7 fintech institutions**: Bivial AG (formerly Klarpay AG), Relio AG, SR Saphirstein AG, Yapeal AG, Mogli AG, SWISS4.0 AG, and Sequence SA. Currently, however, only 5 of these fintech institutions are still in operation. 25 5

Following Mogli AG in 2022, SWISS4.0 AG became another authorized fintech institution that had to be **liquidated** in 2025. According to public information, FINMA had been closely monitoring SWISS4. 0 AG and demanded early measures to improve the startup's financial situation. SWISS4.0 AG and its governing bodies were unable to successfully implement appropriate measures within a reasonable timeframe. On March 4, 2025, FINMA initiated bankruptcy proceedings against the fintech company due to well-founded concerns regarding excessive debt and serious liquidity problems. FINMA appointed Valfor Avocats Sàrl as the bankruptcy liquidator. SWISS4.0 AG was a so-called micro startup with approximately 250 customers. 25 6

Supervision of institutions licensed under Art. 1*b* of BankG remained intensive in 2024 as well. The focus was on protecting depositors due to the institutions' tight capital and liquidity situation. Fintech institutions are generally **startups**, which, as expected, incur high expenses for setup and market entry and initially generate little or no revenue. A successful market entry depends on successful financing rounds and a viable business model. To date, these business models have been exclusively in the area of payment services. The market in this sector is competitive, and margins are low. It has been shown that business models that address a niche with a unique offering or a specialized customer segment can be successful. 25 7

25 8 The market for **payment services** in Switzerland is highly competitive and economically challenging. It is not uncommon for startups to cease operations in such a saturated market. This also explains why just under one-third of the companies licensed under Art. 1*b* of BankG have ceased operations. Furthermore, unlike bank customers, customers of fintech institutions do not enjoy deposit protection. Nor do they benefit from any bankruptcy privilege, even though customer funds are held on the institution's balance sheet. This not only leads to increased default risks for customers and supervisory challenges but also, in a highly competitive environment, reduces the attractiveness of this type of authorization.

25 9 Against this backdrop in particular, **FINMA** is right to require that fintech institutions have ongoing capital and liquidity planning in place and be able to identify bottlenecks in a timely manner. Nevertheless, dangerous situations arose at several institutions in 2024. The situation often worsened due to the questionable recoverability of assets in *Gone -concern* scenarios, when a company was having difficulty continuing its operations and liquidation had to be considered. This particularly affected the valuation of in-house developed software, which often represents a significant asset and can be difficult to sell under time pressure.

VIII. FURTHER DEVELOPMENT OF FINTECH LICENSING

26 0 In its report "Digital Finance: Areas of Action 2022+ ," in Action Area 1, the Federal Council tasked the FDF/SIF, in collaboration with FINMA and with the involvement of the industry, to review the existing legal and supervisory framework with regard to the conditions for new market participants and forms of services.

26 1 FINMA generally assessed the fintech licensing in the context of this review. However, it identified the lack of protection for client funds in the event of bankruptcy as a significant drawback in the existing regulation. Due to this lack of protection, increased demands are placed on supervision, especially since institutions in this sector do not have a stable revenue situation, particularly in the initial phase. Timely monitoring of the institution's financial position is therefore essential. FINMA's supervisory burden for fintech institutions is therefore disproportionately high compared to other supervised entities. FINMA has also identified further weaknesses in the current regulation that complicate supervisory activities, namely the possibility of a limited audit by

the auditing firm (see Art. 1*b*, para. 4, let. b, BankG), the minimum capital requirements, and the provision of ancillary activities by fintech institutions.

Taking a holistic view, the Federal Council considers it appropriate to integrate the solution it is pursuing into the relevant **regulatory efforts**. The proposed solution includes, in particular, better protection of public deposits in the event of the bankruptcy of a 1*b* institution. To this end, the Federal Council considers it necessary to amend financial market regulation to improve customer protection. The lack of **customer protection** applies only to public deposits accepted, but not to the (separable) crypto-based assets that may be accepted under a license pursuant to Art. 1*b* of BankG. 26 2

Note

This publication reflects solely the personal opinions of the authors and does not bind FINMA.

We would like to express our sincere thanks to Dr. Nico Hess for proofreading the manuscript.

BIBLIOGRAPHY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MATERIALS

Bericht des Bundesrates zu Anpassungen des Bankengesetzes vom 15. Juni 2018, abrufbar unter: https://www.efd.admin.ch/dam/de/sd-web/hcvaF5Xv3z-fo/aenderung-bankgesetz-bericht-de.pdf, besucht am 27.4.2026 (zit. Bundesrat, Bericht Bankengesetz).

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

Bundesrat, Bericht vom 16. Dezember 2022 zu Anpassungen des Bankengesetzes vom 15. Juni 2018, abrufbar unter: https://backend.efd.admin.ch/fileservice/sdweb-docs-prod-efdadminch-files/files/2024/04/30/9f-b7f508-2522-428c-a192-23b975c48e93.pdf, besucht am 24.4.2025 (zit. Bundesrat, Bericht 2022).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FINMA, Wegleitung für Gesuche betreffend Bewilligung als Person nach Art. 1*b* Bankengesetz (Fintech-Bewilligung) vom 24. April 2025, abrufbar unter:

https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/w_bewillligungfintech_20250424.pdf?sc_lang=de&hash=DC7EB79EC1BDFD9E6C31C36306DAFA09, besucht am 4.4.2025 (zit. FINMA, Wegleitung Fintech-Bewilligung).