

Innovation, outsourcing and operational resilience

*Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)*

Switzerland has tried to adapt its banking regulation to new business models. Since 2017, the Banking Ordinance has allowed companies to accept public deposits of up to one million francs without a banking licence, provided that they do not invest the deposits or pay interest on them and that they inform their clients that the deposits are not protected. This regime, known as the sandbox, allows start-ups to test their business models before they need a licence.¹

On 1 January 2019, a new licence category followed, which is commonly called the fintech licence. It allows institutions to accept public deposits of up to one hundred million francs, or crypto-assets held in collective custody, provided that they neither invest these funds nor pay interest on them. Since they do not engage in the maturity transformation that characterises a bank, such institutions are subject to lighter requirements. These concern their minimum capital, their organisation and the capital adequacy rules, which are significantly reduced. Their clients enjoy no deposit protection and must be informed of this.² The number of fintech licences granted has remained small. Several holders operate in the field of payments and crypto-assets and digital assets, which explains why the Federal Council's proposals of 2025 for payment instrument institutions and crypto institutions revisited the concept.

As banks outsource more of their activities to service providers and cloud platforms, the supervisor has had to address the resulting risks. FINMA's outsourcing circular, revised in 2018, requires banks to maintain an inventory of their outsourced functions and to select, instruct and monitor their service providers with care. The contracts must ensure that the bank, its audit firm and FINMA retain access to the information they need. When functions are outsourced abroad, the bank must ensure that it can restore them in Switzerland or transfer them to another provider.³

Operational resilience became a supervisory concept in its own right after the Basel Committee adopted its principles on the subject in 2021. FINMA incorporated them into a new circular on operational risks and resilience, which entered into force at the beginning of 2024 and replaced the circular of 2008. Banks must identify their critical functions, define the tolerance for disruption of each function and demonstrate that they can maintain them within these tolerances in severe but plausible scenarios.⁴ The circular also contains requirements for the management of information and communication technology, data and cyber risks.

Cyber attacks are one of the operational risks that FINMA regards as most significant for the Swiss financial centre. Since 2020, supervised institutions must report significant cyber attacks to FINMA within a short period after their detection and submit a full report afterwards. Since 2025, a general reporting obligation for operators of critical infrastructure, which include banks, has also required them to report cyber attacks to the federal cyber security authority.⁵ For a client of a Basel private bank, these rules may appear technical. They protect what matters most to such a client, the confidentiality of data and the availability of assets.

1 Notes

1. On the licence-exempt innovation area (sandbox) for the acceptance of public deposits of up to CHF 1 million under Art. 6 para. 2 Banking Ordinance, in force since 1 August 2017, and the extension of the settlement account exception to 60 days, see SR 952.02 and FINMA publications. To be verified. ↩
2. On the licence for institutions under Art. 1b Banking Act (fintech licence), in force since 1 January 2019, with the threshold of CHF 100 million in public deposits and the facilitated requirements under Art. 14a ff. Banking Ordinance, see SR 952.0, SR 952.02 and FINMA's guidelines. To be verified. ↩
3. FINMA Circular 2018/3 "Outsourcing – banks and insurers", in force since 1 April 2018, on the requirements for the outsourcing of significant functions, including the inventory, the selection and monitoring of service providers, audit and access rights and outsourcing abroad. To be verified. ↩
4. FINMA Circular 2023/1 "Operational risks and resilience – banks", in force since 1 January 2024, replacing Circular 2008/21, and the Basel Committee's Principles for Operational Resilience of March 2021, see the publications of FINMA and the BIS. To be verified. ↩

5. On the reporting obligation for cyber attacks under FINMA Guidance 05/2020 (initial report within 24 hours, full report within 72 hours) and the reporting obligation under the Information Security Act for operators of critical infrastructure, in force since 1 April 2025, see the publications of FINMA and the Federal Office for Cyber Security. To be verified. ↩

For general information only. This article does not constitute legal or tax advice, does not replace advice on an individual case and creates no lawyer-client relationship. It reflects the legal position as of September 2026.

Online version: helveticaregister.com/basel-innovation-outsourcing-and-operational-resilience