

Circular 2023/1: operational risks and resilience

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

FINMA Circular 2023/1 "Operational risks and resilience – banks" of 7 December 2022 entered into force on 1 January 2024 and replaced Circular 2008/21 on operational risks of banks. Its provisions on operational resilience had to be implemented within a transitional period of two years, that is by 1 January 2026.¹ The circular contains requirements on the management of information and communication technology risks, cyber risks, critical data, business continuity management and operational resilience. Institutions must separate development, test and production environments for their IT systems and govern change management (margin nos. 47 to 60). They must identify cyber threats, protect their assets, detect attacks, respond to incidents and recover from them, and they must report successful cyber attacks affecting critical assets to FINMA within 24 hours, followed by a full report within 72 hours (margin nos. 61 to 70).²

The circular defines critical data as data whose importance for the provision of services or for regulatory purposes is so great that they require increased security measures (margin nos. 71 to 82).³ Client data used to train or operate an artificial intelligence system will often be critical data in this sense. Business continuity management requires recovery time and recovery point objectives, continuity and disaster recovery plans and regular tests (margin nos. 83 to 96). The concept of operational resilience, finally, requires institutions to identify their critical functions and to define "tolerances for disruption", the maximum disruption of a critical function that the institution can accept under severe but plausible scenarios, and to test them regularly (margin nos. 97 to 114).⁴

For a Lugano bank, the operational resilience requirements meant identifying which functions, such as payments, custody and client access, are critical, and mapping the people, processes, technology, information and providers on which they depend. Where an artificial intelligence

system has become part of a critical function, for example a monitoring system without which payments cannot be released, the institution must plan for its failure: a fallback to manual processes, an alternative provider or a reduced service. The documentation of fallback solutions that FINMA requires in Guidance 08/2024 is the link between the two sets of rules.⁵

1 The reporting obligation for cyber attacks under the Information Security Act

Since 1 April 2025 operators of critical infrastructures in Switzerland have been required to report cyber attacks to the National Cyber Security Centre, which became the Federal Office for Cyber Security (BACS) in 2024. The obligation was introduced by an amendment of the Information Security Act and applies, among others, to banks, insurance companies and financial market infrastructures. Reports must be made within 24 hours of the discovery of an attack that endangers the functioning of the infrastructure, has led to the manipulation or outflow of information, has remained undetected for a long period or is associated with blackmail, threats or coercion. Violations of the reporting obligation have been punishable by fines of up to CHF 100,000 since 1 October 2025.⁶ Financial institutions supervised by FINMA must therefore coordinate two reporting channels, the report to FINMA under Circular 2023/1 and the report to the BACS under the Information Security Act. The federal authorities have provided for a common reporting form so that a single report can serve both purposes.⁷

2 Notes

1. FINMA Circular 2023/1 "Operational risks and resilience – banks" of 7 December 2022, <https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?la=en>. ↩
2. FINMA Circular 2023/1 (above), margin nos. 47–70. ↩
3. FINMA Circular 2023/1 (above), margin nos. 71–82. ↩
4. FINMA Circular 2023/1 (above), margin nos. 83–114. ↩
5. FINMA, Guidance 08/2024 (above), section 2.5. ↩
6. Federal Act on Information Security at the Confederation of 18 December 2020 (Information Security Act, ISA), SR 128, Art. 74a–74h and 74e (sanctions), as amended by the Federal Act of 29 September

2023; Cybersecurity Ordinance of 7 March 2025 (CSO), SR 128.51. In force since 1 April 2025, sanctions applicable from 1 October 2025. ↩

7. Federal Office for Cyber Security (BACS), information on the reporting obligation and the reporting form. ↩

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/lugano-circular-2023-1-operational-risks-and-resilience