CENTRE DE DROIT
BANCAIRE ET FINANCIER

**FINMA supervision**

# A new circular on operational risks

Par Célian Hirsch le 19 December 2022

New international standards and strong developments in the field of digitalization. These are the two factors cited by FINMA to justify the revision of its Circular 08/21 on operational risks. Adopted on December 7, 2022, Circular 2023/1 will come into force on January 1, 2024.

The new circular distinguishes between the global management of operational risks and the management of specific operational risks. The latter include those related to information and communication technologies (ICT), cyber risks, critical data and, finally, cross-border service activities. This commentary focuses on the first three types of risk, before briefly touching on a new feature of the circular : operational resilience.

Operational risks correspond to the risk of “financial loss resulting from the inadequacy or failure of internal processes or systems, from inappropriate actions or errors by individuals, or from external events”. The definition corresponds to that of art. 89 of the Capital Adequacy Ordinance and that of the Basel Committee on Banking Supervision (BCBS). The central element is that of financial loss, which is understood in a broad sense. This includes, for example, cyber attacks that result in a loss of customer confidence, even if the financial loss is not directly quantifiable.

Digital evolution means that those subject to the law need to manage changes to their ICT (change management), its operation (run, maintenance) and incident management. With regard to the first aspect, taxable persons must in particular guarantee the separation between development or test environments, on the one hand, and the ICT production environment, on the other. With regard to the second, the licensee must have an inventory that includes hardware and software components, as well as critical data backup locations. Finally, in the event of a major ICT incident, the reporting entity must inform FINMA without delay.

Cyber-risk management also imposes a duty to inform FINMA of cyber-attacks, but this duty is not new (and will probably be reviewed in the near future to adapt to a future more general obligation to report cyber-attacks). The main obligation lies in the implementation of a strategy against cyber attacks. This strategy must include processes and controls to (a) identify specific and potential cyber-attack threats, (b) protect the confidentiality, integrity and availability of critical electronic data and ICT components, (c) rapidly detect cyber-attacks and, finally, (d) respond to vulnerabilities and (e) rapidly restore business operations following a cyber-attack. In addition, the insurer must carry out penetration tests and cyber exercises.

In Appendix 3 of Circular 08/21, FINMA imposed special protection for “customer identification data” (CID). The emphasis was placed on the confidentiality of this data alone. In line with technological developments, protection now applies to all important data in terms of confidentiality, integrity and availability (but not in terms of traceability).

Circular 23/1 thus imposes special protection on so-called “critical information assets” (according to BCBS terminology). Whereas the draft circular provided for a broad definition of “critical data”, a definition close to that proposed by the Swiss Bankers Association has been adopted. Critical data are “data which, in view of the size, complexity, structure, risk profile and business model of the institution, are of such importance that they require increased security requirements”. It is up to each institution to identify its critical data.

Once identified, this data is subject to special protection measures. These measures include not only limited access by employees (need-to-know principle) and employee training and monitoring, but also protection and monitoring of data when stored outside Switzerland, and due diligence of service providers who process such data. Finally, any significant incident involving critical data must be reported immediately to FINMA.

Finally, Circular 23/1 contains requirements for operational resilience. The inclusion of these requirements is justified by the increase in “operational shocks”, such as pandemics, cyber-attacks, systemic failures, supply chain breakdowns, widespread or sustained power cuts, or natural disasters.

Operational resilience has also been the subject of new regulations at international level. In March 2021, the BCBS adopted its Principles for operational resilience. More recently, in November 2022, the Council of the European Union approved the Regulation on digital operational resilience in the financial sector (DORA Regulation, see cdbf.ch/1164/). Its entry into force will be phased in over two years, like the rules on resilience in Circular 23/1. However, unlike Swiss law, the DORA regulation applies not only to financial entities, but also to third-party providers of ICT services, such as cloud providers.

---