Grant Thornton

New FINMA circular “Operational risks and resilience”

FINMA Circular 2023/1 “Operational risks and resilience – banks” comes into force on 1 January 2024. When the revised FINMA Circular comes into force, significant adjustments will be made in the areas of information and communication technology (ICT) risk management and critical data risk management. New requirements for ensuring operational resilience must also be observed. What are the most important aspects of the circular and what significance does it have for FinIA institutions?

Classification[1]

	Banks / Securities firms	**Asset management institutes** (fund management companies, managers of collective assets)	**Asset managers / trustees**	**Other financial intermediaries** (SRO[2]-supervised)
Applicability	Yes	Indirect	Indirect	No
Relevance	High	Partial	Partial	Low

[1] This is a highly simplified presentation intended to enable a quick initial categorisation of the topic. Each institution should determine the relevance and the specific need for action individually and specifically.
[2] Self-regulatory organisation (SRO)

Background

The new circular focuses on the importance of operational risks and resilience for financial institutions. It is intended to take account of the structural change and an increasing threat situation in relation to ICT risks. This includes technical developments such as progress in digitalisation, increasing complexity of supply chains and dependencies as well as the increase in cyber-attacks. Other drivers for the revision of the circular were international regulatory developments.

Innovations in the area of operational risk management

The requirements of the Circular on the management of operational risks are divided into the following areas:

- Overarching management of operational risks
- ICT risk management (information and communication technology)
- Cyber risk management
- Critical data risk management
- Business Continuity Management (BCM)
- Management of risks from the cross-border services business (cross-border)

The content of these areas of the FINMA Circular was revised or updated to varying degrees. Some have remained completely unchanged, while others have undergone significant changes.

An already familiar focus of the FINMA Circular is the management of operational risks. FINMA has now summarised the overarching management of operational risks in one chapter in order to make supervisory expectations more transparent. The content has remained unchanged.

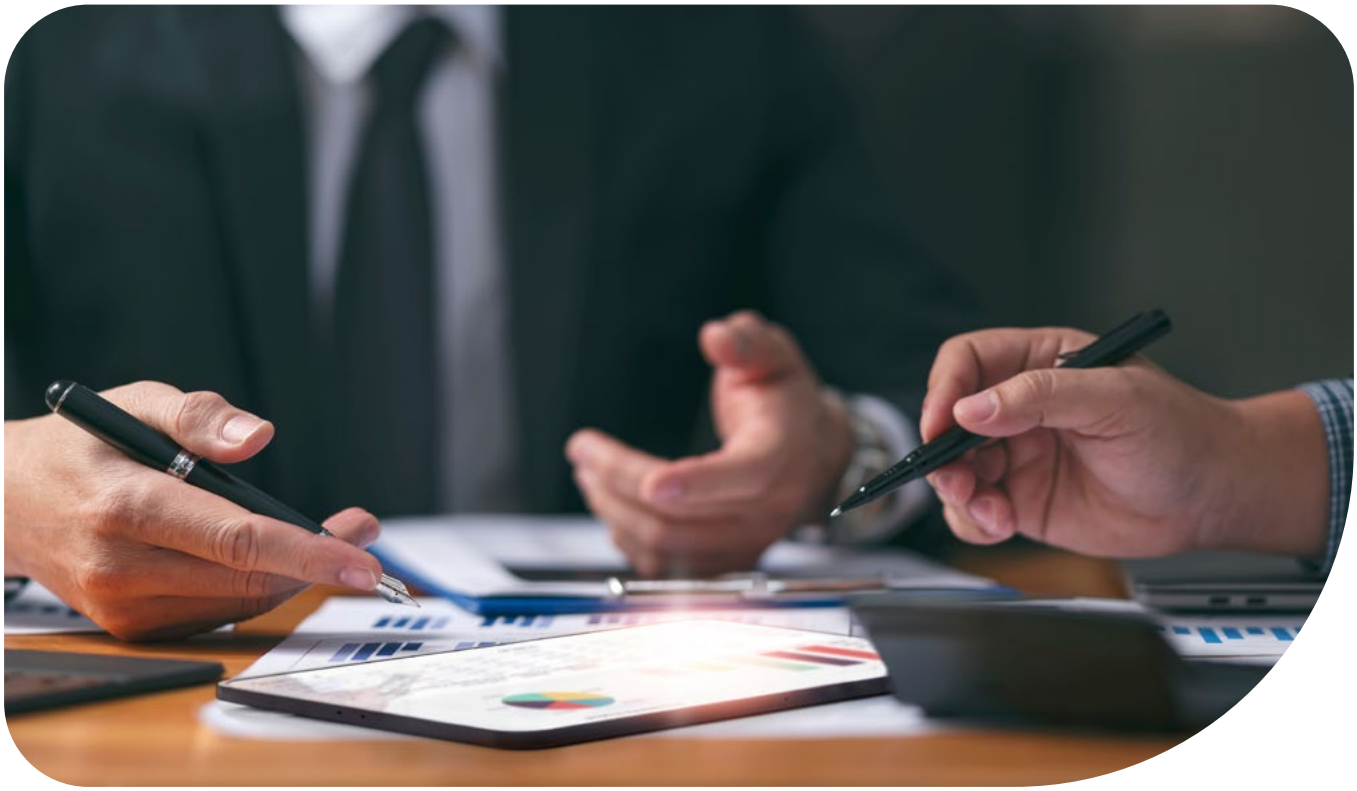
In the area of ICT risk management, significant adjustments were made based on the Principles of Operational Resilience (POR) developed by the Basel Committee on Banking Supervision and the revised Principles for the Sound Management of Operational Risk (PSMOR).

Further significant adjustments were made to the regulation of critical data risk management. The circular now contains a definition of the term “critical data”. The term has been expanded to include all data that are of such crucial significance to the institution that they require increased security measures.

The new chapter on Business Continuity Management (BMC) in the circular replaces the previous SBA self-regulation. The regulation on BCM was updated when it was incorporated into the circular. Minor adjustments were made to the chapter on cyber risk management. The management of risks from the cross-border services business and the continuation of critical services in the resolution and reorganisation of systemically important banks in Chapter VI remain unchanged.

Operational resilience

The circular now focuses on ensuring operational resilience and contains related requirements in a separate chapter V. Operational resilience refers to the ability of an institution to restore its critical functions in the event of disruptions within the tolerance for disruption. A holistic approach is expected that records, monitors, and reports on both preventive and reactive measures in their entirety.



FINMA's expectations based on on-site inspections carried out

During on-site inspections in the run-up to the entry into force of the FINMA Circular, FINMA identified areas for improvement at many institutions, such as currentness and completeness of the ICT inventory. FINMA also found that some institutions did not systematically monitor their technological infrastructure in a timely and systematic manner. FINMA furthermore noticed that the focus in the identification of critical data is sometimes closely limited to client identifying data (CID), whereas a broader approach is expected under the new circular when assessing and determining the criticality of data.

Applicability and significance for FinIA institutions

The circular is only directly applicable to banks, financial groups and conglomerates and securities firms. The requirements are limited by FINMA by exempting banks and securities firms in supervisory categories 4 and 5 from the obligation to fulfil numerous marginal points. The implementation of the FINMA Circular also depends on various factors in individual cases, such as the size, complexity, structure, and risk profile of the bank in question. Depending on the situation, FINMA may relax or tighten rules. Transitional provisions of up to two years apply in some cases to the new chapter on operational resilience. The other areas of the circular will enter into force on 1 January 2024 without transitional provisions.

Except for banks and investment firms, the Circular is not aimed at other FinIA institutions and is therefore not directly applicable to them. Nevertheless, the circular contains numerous FINMA expectations which, to a lesser extent and depending on the size, complexity, structure, and risk profile of the institution, are also likely to apply to lower regulated institutions. This includes, for example, many general requirements on operational risk management or requirements around cross-border risk. FinIA institutions should also not ignore the marginal points on cyber risk management and BCM.

Conclusion and outlook

FINMA Circular 2023/1 contains important new and stricter requirements in relation to the management of operational risks and operational resilience at financial institutions. Due to the reasonable lead time, banks and securities firms should have prepared and implemented most of the adjustments resulting from the FINMA Circular in order to be ready for its entry into force. The next challenge for them will be the specific implementation in practice, in particular of the procedures, processes, and controls. Although other FinIA institutions are not directly affected, they should clarify the extent to which the circular is relevant or helpful for them, depending on the size, complexity, structure, and risk profile of their institution.

Fabian Schmid
Partner, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 50
E fabian.schmid@ch.gt.com

Christopher Oehri
Partner, Advisory IT & Digitalisation
Grant Thornton AG
T +423 237 42 10
E christopher.oehri@ch.gt.com

Nina Helbling
Senior Accountant, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 58
E nina.helbling@ch.gt.com

Grant Thornton