FINMA Circular 2023/1

"Operational risk and resilience – banks"
Specific implementation challenges for the board of directors

In December 2022, FINMA published the fully revised circular on operational risk and resilience, which will enter into force on 1 January 2024 and replace the previous circular. The new publication also specifies and extends the requirements for the board of directors. Banks should begin to identify any gaps in their organizational structure, risk processes and control system in order to comply with the circular on time. Although implementation will require considerable effort, the operational resilience requirements are also an opportunity for banks.

Background and key points

The current Circular 2008/21 on operational risk came into force in 2009. In publishing the new circular, FINMA is responding to the increased risk situation. The circular also addresses rapid developments in digitalization and information and communication technology (ICT). In addition, it implements revised requirements of the Basel Committee on Banking Supervision (BCBS) on the sound management of operational risks as well as the new Basel principles for operational resilience.

The new FINMA requirements reflect three aspects. First, they provide concrete guidance on previous supervisory practice in the areas of risk governance and strategy, cyber risks and crisis management. Second, the requirements for dealing with critical data and ICT risks have been significantly expanded. And third, operational resilience requirements have been added.

“Considerable effort is needed to implement the new FINMA requirements.”

FINMA defines operational resilience as the institution’s ability to build its operating model in such a way that it can protect itself against threats and failures and, in the event of an incident, restore its critical functions within predefined interruption tolerances. For FINMA, critical functions include the activities, processes and services whose disruption would jeopardize the institution’s continuation or its role on the financial market. To protect critical functions, banks must take an end-to-end view of the entire value chain, including dependencies on resources, systems and external service providers.

In principle, all banks are subject to the new requirements, although FINMA provides extensive relief for smaller banks by applying the principle of proportionality.

The new circular also specifies and expands the role and responsibilities of the board of directors with regard to strategic risk management and monitoring.

Role and responsibilities of the board of directors under the new circular

As the ultimate governing body, the board of directors is primarily called upon to act with regard to the first and third aspects. For example, the board of directors has to approve guard rails in the form of internal guidelines on operational risk management and strategies for dealing with ICT, cyber risks, critical data and business continuity management (BCM). The board is also required to monitor compliance with these guidelines.

At the risk strategy level, the board of directors must approve the risk tolerance for operational risks at least once a year, taking into account the effectiveness of risk and control measures as well as the institution’s strategic and financial goals. Risk tolerance must be set not only for residual risks, i.e. risks remaining after risk mitigation measures and controls, but also for inherent risks. To this end, the board of directors must consider strategic decisions relating to the business or operating model. For example, this means deciding whether certain customer segments or countries should be served at all, or whether certain products should be offered. Depending on the risk tolerance, the board of directors then makes any necessary strategic adjustments such as amendments to the business model.

In the area of BCM, the circular incorporates and updates the recommendations of the Swiss Bankers Association (SBA), which are recognized as self-regulatory. Some previous SBA recommendations relating to the board of directors, which were not minimum standards, are now specified in the circular. These include ensuring the accessibility of responsible persons in crisis situations and regular reporting of BCM activities to the board of directors.

The board of directors is also involved when it comes to the third aspect: operational resilience. In determining critical functions, FINMA expects a top-down view of strategically important operations and service delivery, i.e. critical functions. Accordingly, the board of directors must approve the bank's critical functions and their tolerances for interruption at least annually. While banks can typically be assumed to have few critical functions, there is at least one at each bank, e.g. payment transactions. The board of directors must also monitor the procedure for ensuring operational resilience. In order to do so, the board should receive reports on the subject at least annually – but also in the event of any incidents.

Challenges facing the board of directors

The challenges for the board of directors are primarily at the levels of risk strategy and organization.

If the board of directors is to meet the risk strategy requirements placed upon it, it must have appropriate expertise in the areas of operational risk management, internal control systems, ICT and cyber risks, and crisis management, as well as a good understanding of the critical functions and associated interdependencies. In many banks, there is significant asymmetry in the know-how and information available to the board of directors and the bank's operational management.

A further complication comes from the lower maturity of operational risk management at many banks compared to financial risk management. At the same time, the process for identifying and assessing operational risks and the criteria for defining tolerances for inherent and residual risks are often less formalized. This is especially true in the areas of ICT, cyber risks and handling of critical data. This in turn makes it more difficult for operational risk management to define risk-mitigating measures and effective controls, which can result in fragmented operational risk reporting that fails to address the needs of the target audience. It means the board of directors lacks a holistic view of the risk situation, critical functions and resources, as well as their dependencies on external partners – information it needs in order meet FINMA's requirement to align the risk situation with the business strategy.

As an additional challenge, an end-to-end view must now be taken across critical functions and implemented as an integrated element throughout the organization and across all lines of defense. This demands solid anchoring in risk and crisis management and bank-wide harmonization of the functions responsible for managing operational resources. This is complicated by the fact that at many banks the tasks, competencies and responsibilities in the area of operational risks have often grown historically. It means that segregation between the operational units and risk control is not always clear.

Experience to date shows that considerable effort is needed to implement the new FINMA requirements – particularly in the areas of risk control, ICT, handling of critical data, operational resilience, crisis exercises and internal reporting. Organizational units such as IT and risk control therefore face major challenges in implementing the changes in a timely manner and managing the expected additional work on the operating side.

At the organizational level, the board of directors and management will be required to ensure clear risk governance in the area of operational risks, which enables end-to-end risk management and control. In parallel, the necessary financial and human resources must be made available for implementation and operation.

Recommended next steps

The board of directors should actively address the topic of operational risk management and operational resilience. Regular training on these topics is recommended in order to meet this need.

At the risk strategy level, the board of directors and management should start identifying any gaps and potential for improvement in governance, the bank-wide risk process and the control system so that the bank can comply with the circular in a timely manner.

The board of directors should also review and critically question whether it has suitable and timely information at its disposal to fulfill its monitoring function and inform risk strategy decisions. If not, it is advisable to adjust risk reporting and especially to have it integrated with the rest of the bank's risk reporting. That way, the board can obtain a holistic view of the risk profile and how it compares with risk tolerances. Often, synergies in the reporting process can also be realized, enabling reports that have grown over the years to be streamlined.

With regard to the organizational challenges, the management should present its plan for implementation of the FINMA circular to the board of directors. In particular, this should outline the financial and human resources required for implementation and subsequent operations. During implementation or, at the latest, in the course of ongoing operations, it is advisable to review regularly whether efficiency gains can be realized by means of system support (e.g. the introduction of a governance, risk and compliance solution), adjustments to the operating model (digitalization strategy, automation) or outsourcing.

To achieve operational resilience, the board of directors needs to engage in active dialog with management at an early stage so that critical functions can be defined. The board should also demand transparency on interruption tolerances and possible failure scenarios. In doing so, it must understand key dependencies on thirdparties in its assessment and consider the impact on reputation and other risks, such as liquidity risks.

Opportunities offered by the new FINMA circular

The requirements for operational resilience also offer opportunities. The concept of operational resilience is not new, and has long been used by companies that rely heavily on operational stability such as hospitals, power plants and air traffic control centers.

For a company to become operationally resilient, it must – on the technical side – be highly familiar with its processes, systems, resources and associated dependencies. It needs to master and optimize these on an ongoing basis. At the same time, companies can increase their resilience by establishing a culture of resilience. This includes a strong risk and error culture, a high level of sensitivity to operations, and the desire to achieve operational excellence.

Resilient companies not only respond better in a crisis; they often also work more efficiently – and therefore more cost-effectively – during normal operations. Ensuring operational resilience, then, is also an opportunity to drive improvements and operating excellence, and to generate competitive advantages.

Dr. Hans Ulrich Bacher
Director, Financial Services
KPMG Switzerland

+41 58 249 51 63
hbacher@kpmg.com

Hanna Read
Manager, Financial Services,
KPMG Switzerland

+41 58 249 28 33
hannaread@kpmg.com