Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

# FINMA Guidance 05/2025

## Operational resilience for banks, persons under Article 1*b* BA, securities firms and financial market infrastructures

10 November 2025

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

finma

# Contents

# 1 Introduction

Banks, persons under section 1b of the Banking Act of 8 November 1934 (BA; SR *952.0*), securities firms and financial market infrastructures must provide for appropriate risk management within the scope of their business activities. Risk management must cover all business activities and be organised in such a way that all material risks can be identified, assessed, controlled and monitored. Against the backdrop of various growing risks in the financial markets and new operational challenges (including cyber attacks), FINMA has increasingly focused not only on operational risks in general, but also on the operational resilience of institutions in particular.

In the various supervisory provisions, operational resilience refers to the institution's ability to restore its critical functions in case of a disruption within the tolerance for disruption. It is the institution's ability to identify threats and possible failures, to protect itself from them and to respond to them, to restore normal business operations in the event of disruptions and to minimise the impact of disruptions on the provision of critical functions. Operational resilience thus reduces not only the residual risks of disruptions, but also the inherent risk of disruptions occurring.

The financial sector today is highly interconnected and interdependent. This connectedness results in a concentration of risks. A disruption in one area can therefore have far-reaching effects on other parts of the financial system. Operational resilience is consequently of crucial importance for protecting the proper functioning of the financial markets. FINMA's focus on the operational resilience of financial institutions thus not only strengthens the protection of creditors, but also the proper functioning of the financial markets as such and is consequently fundamental to a strong financial market system.

This guidance is based on the findings of a data survey conducted by FINMA as at 31 December 2024 among 267 banks, securities firms, financial groups and financial market infrastructures (hereinafter "institutions") on the topic of ensuring operational resilience.

The purpose of the guidance is to raise awareness of the subject of operational resilience so that the various regulatory requirements can be effectively implemented and operational resilience to growing threats and operational shocks strengthened in a targeted manner.

## 2 Legal framework

For banks and for persons under Article 1*b* BA, the obligation to identify, limit and monitor their risks arises primarily from the organisational requirements pursuant to Article 1*a* and Article 1*b,* and Article 3 para. 2 let. a and Article 3*c* BA in conjunction with Article 12 para. 2 and Article 14*e* of the Banking Ordinance of 30 April 2014 (BO; SR *952.02*).

For securities firms, this obligation essentially arises from Article 9 para. 2, Articles 41 and 49 of the Financial Institutions Act of 15 June 2018 (FinIA; SR *954.1*) and Article 12 para. 4 and Article 68 of the Financial Institutions Ordinance of 6 November 2019 (FinIO; SR *954.11*). For financial market infrastructures, the obligation is based on Article 8 para. 3 of the Financial Market Infrastructure Act of 19 June 2015 (FinMIA; SR *958.1*) and Article 9 para. 1 let. d of the Financial Market Infrastructure Ordinance of 25 November 2015 (FinMIO; SR *958.11*).

FINMA has set out its supervisory approach on this matter in Circular 2023/1 “Operational risks and resilience – banks”.

## 3 Findings from the data survey

The 267 institutions surveyed by FINMA rated the maturity of their own operational resilience on a scale of 0–10[1] at 7.5 (mean value) and that of the Swiss financial sector as a whole at 6.7 (mean value). Selected findings from the data survey to ensure operational resilience are presented below.

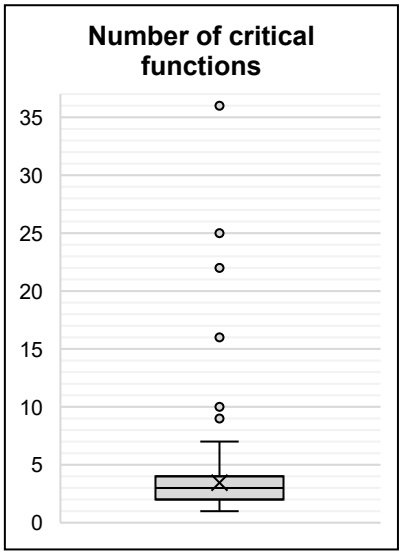
### 3.1 Critical functions[2]

**Findings**

The following chart displays the number of critical functions defined by the institutions in aggregate form. FINMA has observed that the number of critical functions is between 1 and 36, with half of the institutions having defined no more than 3 critical functions (median). At the same time, the middle half identify between 2 and 4 critical functions. The arithmetic mean is around 3.5 critical functions.

[1] Self-assessment by the institutions on a scale of 0 to 10; where 0 = not resilient and 10 = absolutely resilient.

[2] See margin nos. 14–16, FINMA Circ. 23/1.

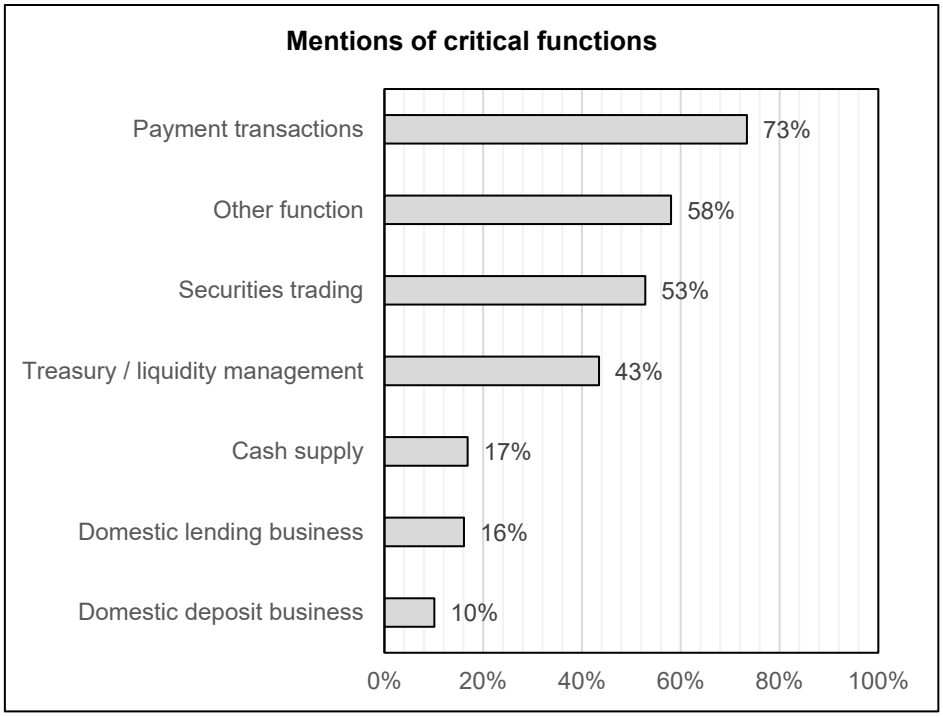



In the “normal range”, institutions identified at least one single critical function, while the largest number observed is 7 critical functions. In addition, the boxplot shows several outliers from 9 to 36 critical functions.

The underlying data allows a statement to be made on the correlation between the number of critical functions and the size and complexity of the institution. It can therefore be concluded that large, complex institutions have defined a higher number of critical functions and vice versa.

To summarise, it was found that the middle half of the institutions identified between 2 and 4 critical functions and that the number increases with the size and complexity of the institution.

The type of critical functions identified depends particularly on the respective business model of the institution. The following bar chart shows the frequency of responses to the survey on the type of critical functions, with multiple answers possible.



FINMA notes that the institutions most frequently identified “payment transactions” as a critical function from the predefined response options (73%) and that “domestic deposit business” was mentioned least frequently. In addition to the predefined response options, the institutions recorded around 300 responses as free text under “Other function”. Around two-thirds of these responses (e.g. postal services, telephone switchboard, IT operations, back office) are not critical functions within the meaning of FINMA Circ. 23/1, margin nos. 14–16, but processes, activities or underlying resources.[3] At the same time, 71% of all critical functions mentioned are directly or indirectly dependent on services provided by third parties.

**Notes**

With 1 to 7 critical functions, the majority of institutions have limited themselves to a small and easily manageable number[4] of critical functions, which is in line with regulatory requirements. In the case of institutions with more than 7 critical functions – as cited by individual institutions –, the number of such functions must be questioned. Among other things, it raises the question of whether 25 or 36 critical functions can be monitored and operated in a resilient manner, or whether the operation of such a high number of critical functions is justifiable from a business perspective. Due to the high proportion of critical functions dependent on third parties, an end-to-end or front-to-back view of the entire supply chain required for their provision and the resources needed for this is particularly important.[5]

The nature of the critical functions reflects an institution’s business model and must be clearly distinguished from processes, activities and underlying resources. Around two thirds of the critical functions mentioned in the free text are to be critically reviewed in light of FINMA Circ. 23/1. For example, regulatory reporting, ensuring due diligence in the area of conduct issues, risk management and risk control, client management, accounting, front and back office activities and representation activities are central components of business activities. They are not, however, critical functions within the meaning of FINMA Circ. 23/1, but are processes and must be classified as such accordingly. Neither do the core banking system, for example, the IT infrastructure and IT operations as well as telephony represent critical functions from a strategic perspective, but are to be classified as underlying resources. Other responses, such as connectivity, system availability and

---

[3] See also the explanatory notes of 7 December 2022 on Circular 2008/21 “Operational risks – banks” – full revision and Circular 2013/3 “Auditing” – partial revision, section 4.1.8 Operational resilience (chapter V), pages 20–25, available at www.finma.ch > Documentation > Consultations and evaluations > Completed consultations > 2022 > FINMA Circular 2008/21 “Operational risks – banks” – full revision (10.05.2022–11.7.2022) (hereinafter “Explanatory notes on FINMA Circ. 23/1) (only available in German).

[4] See explanatory notes on FINMA Circ. 23/1, page 22.

[5] See explanatory notes on FINMA Circ. 23/1, page 22.

accessibility, are merely parameters for monitoring the inventory of critical functions.

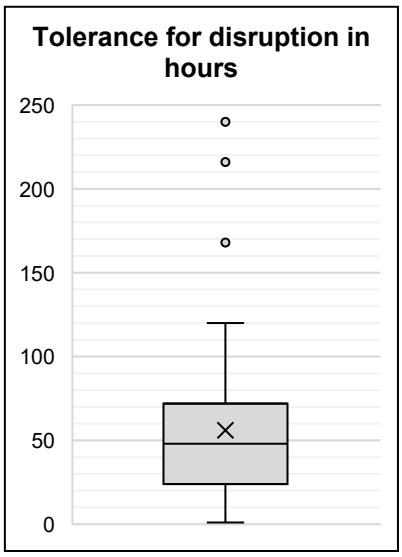
The processes and underlying resources serve the overriding purpose of providing critical functions. Therefore, the failure of a critical function always has a direct and immediate impact on the “clients” of an institution, on the “institution” itself or on the “proper functioning of the financial markets” as a whole. When identifying the critical function, a top-down strategic view should be adopted and accordingly only the strategically most important operations or services should be defined as critical functions.

In the inventory of critical functions, the underlying processes, underlying resources and their interdependencies must be presented in addition to the critical functions. A table without internal dependencies does not constitute an inventory of critical functions within the meaning of margin no. 107, FINMA Circ. 23/1.

## 3.2 Tolerances for disruption

**Findings**

The following chart summarises the tolerance for disruption of all critical functions of the surveyed institutions in hours. It shows that the majority of institutions have chosen a time-based measurement for the tolerance for disruption. Only in a few cases was the cancellation and error rate or a lower threshold value for “liquid assets”, for example, defined as a tolerance value instead of time.




The tolerances for disruption range between 1 and 8,736 hours (365 days),[6] with half of all institutions defining a tolerance of no more than 48 hours (median). At the same time, the middle half of all responses is between 24 and 72 hours. The arithmetic mean is 56 hours.

The underlying data shows no correlation between the tolerances for disruption and the size and complexity of the respective institution. The

[6] In accordance with FINMA Circ. 23/1, functions with a tolerance for disruption of more than 10 days / 240 hours must be checked for criticality. For evaluation purposes and to improve readability, all values over 10 days / 240 hours were removed from this boxplot chart and are also not included in the average calculations.

tolerance for disruption is defined according to the type of critical function and the impact on it, as required by supervisory provisions.

To summarise, it was found that the middle half of the institutions defined tolerances for disruption of between 24 and 72 hours and that these are independent of the size or complexity of the institution.

Furthermore, in the course of its supervisory activities and the *Horizontal Reviews of Operational Resilience 2025*,[7] FINMA found that the tolerances for disruption for institutions in supervisory categories 1 to 3 were partly defined on the basis of the recovery capabilities of the institution following a serious but plausible scenario (reverse engineering) and not on the basis of the tolerance readiness of the executive board.

**Notes**

In addition to the time dimension, other metrics such as financial loss, client loss, etc. can also be used to define the tolerances for disruption. The anticipated effects on the “client relationship”, the “institution” itself and the “proper functioning of the financial markets” as a whole are of central importance.

The supervisory requirements stipulate that the tolerances for disruption must reflect the tolerance of the executive board to shocks – irrespective of the institution’s ability to recover.[8] Reverse engineering is at odds with the supervisory provisions.

Outliers with tolerances for disruption of less than 24 hours should be scrutinised. On the one hand, it must be checked whether these are actually critical functions within the meaning of FINMA Circular 2023/1 (see section 3.1) or critical processes whose tolerances are defined as part of business continuity management (BCM) in the form of RTO/RPO.[9] On the other hand, it must be checked whether the definition and calibration of the tolerance for disruption is appropriate and whether the dimensions of “client relationship”, “continuation of the institution” and “proper functioning of the financial markets” have been adequately taken into account.

In the case of low defined tolerances for disruption, the dependency on external service providers and suppliers in particular must be critically examined and transparent communication of the tolerances throughout the entire supply chain must be ensured. When defining the tolerance for disruption, an end-to-end or front-to-back view of the entire supply chain

---

[7] Not all *Horizontal Reviews of Operational Resilience 2025* have been concluded as at the date of publication of this guidance.

[8] See margin no. 101, FINMA Circ. 23/1.

[9] RTO/RPO stands for recovery time objective (RTO) / recovery point objective (RPO); see margin no. 10, FINMA Circ. 23/1.

must be adopted and the resources required for this must be taken into account.[10]

Tolerances for disruption of over 240 hours (10 days), however, are very high. A function that clients, the institution and the financial markets can do without for more than 10 days – without partial recovery, alternative fallback systems, workarounds, etc. – may not be critical for the institution. FINMA suggests that these high tolerances for disruption be reviewed the next time they are due to be approved by the executive board.

Tolerances for disruption of over 120 hours (5 days) should also be questioned. This raises the question of whether a client relationship or the institution itself would survive such a high tolerance. When defining the tolerances for disruption, it is also possible to define a lower tolerance for disruption than the institution's current recovery capability. In such a case (out of tolerance), measures must be taken to ensure operational resilience in order to enter the tolerance range.

## 3.3 Testing

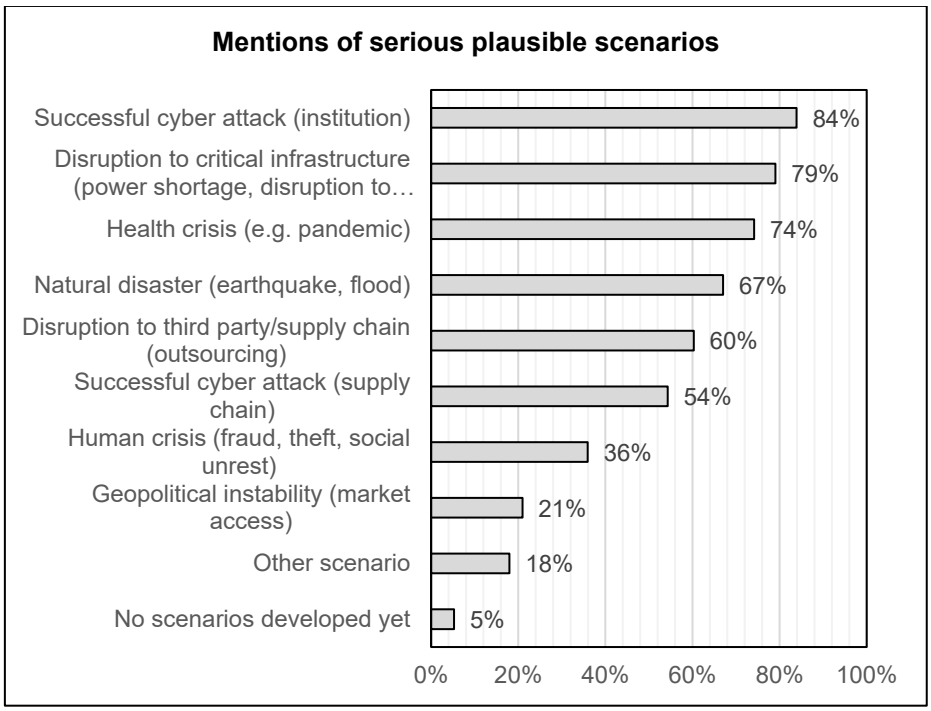
**Findings**

Testing serves to identify weaknesses and thus improve operational resilience. FINMA notes that 85% of institutions in supervisory categories 1 to 3 have not yet carried out any testing at the time of the data survey.

10% of institutions have already scheduled testing, of which the clear majority (72%) are planning annual testing in the future. The remaining 5% of institutions have neither tested nor included this in their future plans.

The following bar chart shows the serious but plausible scenarios that the institutions listed in the predefined response options for the testing.

[10] See explanatory notes on FINMA Circ. 23/1, page 22.




In the data survey, 84% of institutions cited a “successful cyber attack” as a serious but plausible scenario for their testing. The scenario of a “Successful cyber attack (supply chain)” was cited by 54% of respondents. The “Disruption to third party/supply chain (outsourcing)” scenario was also listed with a frequency of 60%. Of those surveyed, 18% defined other scenarios; 5% of the institutions have not yet developed any scenarios.

**Notes**

Institutions in supervisory categories 1 to 3 must carry out regular testing.[11] The ability to provide critical functions within their tolerances for disruption in severe but plausible scenarios is tested.

When planning and organising the testing, an end-to-end or front-to-back view of the entire supply chain and the resources required for this must be taken.[12] A cross-institution test or testing in conjunction with other institutions may offer advantages. In addition, the entirety of all elements to be tested must be visible to the executive board in order to enable an independent assessment of the framework for operational resilience.[13]

[11] See margin nos. 20 and 110, FINMA Circ. 23/1.

[12] See explanatory notes on FINMA Circ. 23/1, page 22.

[13] See margin no. 103, FINMA Circ. 23/1.

FINMA emphasises that supervised institutions must develop serious but plausible scenarios for the testing on the basis of the institution-specific potential threats.[14] In particular, the threat and vulnerability analysis from non-cyber activities should be developed further, as it does not yet have the required level of maturity at some institutions.

## 3.4 Framework for operational resilience

**Findings**

FINMA notes that, according to the data survey, coordination of the the existing relevant components[15] to strengthen operational resilience is only taking place at 12–15%[16] of the institutions surveyed in supervisory categories 1 to 3 and has therefore not yet been fully implemented in the market.

In order to monitor operational resilience and the framework implemented with it, around 60% of all institutions surveyed use their own parameters and indicators.[17] The number of indicators per institution varies from one indicator to 31 defined parameters in order to monitor and manage operational resilience.

**Notes**

From 1 January 2026, institutions in supervisory categories 1 to 3 must coordinate the framework for ensuring operational resilience with other relevant components such as the management of operational risks, including the management of ICT and cyber risks, business continuity management (BCM), the management of third parties and emergency planning in order to strengthen their operational resilience in the long term.[18]

This encompasses an appropriate exchange of relevant information between the relevant components. This exchange of information and the definition of relevant parameters are basic prerequisites for the effectiveness of the measures taken to ensure operational resilience.[19] This enables the

---

[14] See margin no. 70, FINMA Circ. 23/1, in conjunction with FINMA Guidance 03/2024.

[15] Management of operational risks, including the management of ICT and cyber risks, business continuity management (BCM), management of third parties and emergency planning.

[16] Depending on the respective supervisory component.

[17] E.g.: End-of-life monitoring, system availability of the core banking system, IT stability: cumulative downtime / unplanned outages, number of critical vulnerabilities, proportion of overdue vulnerability management, number of SOC incidents, number of failed cyber key controls, number of DLP events, number of cases exceeding defined RTO/RPO, number of overdue major incidents, number of overdue audit violations/measures, number of loss events, number of activated BCP plans, violations of service level agreements (SLAs) for key outsourcing, number of key personnel losses.

[18] See margin nos. 104 and 113, FINMA Circ. 23/1.

[19] See margin nos. 102 and 113, FINMA Circ. 23/1.

effectiveness of the framework to be monitored and the operational resilience of the institution to be assessed using independent indicators.

## 4 Conclusion and next steps

As part of its supervisory activities, FINMA emphasises the importance of institutions being operationally resilient on the basis of the supervisory requirement of appropriate risk management. In particular, the focus is on the resilience of critical functions, regardless of the size and complexity of the respective institution.

The findings from the data survey, the regular supervisory discussions and the *Horizontal Reviews of Operational Resilience 2025*[20] currently still show a very heterogeneous picture with regard to the interpretation of the supervisory requirements, the implementation status and the degree of maturity of operational resilience at the supervised institutions.

From 1 January 2026, institutions, regardless of their supervisory category, must take measures to ensure operational resilience, taking into account serious but plausible scenarios.[21] These measures are expected to improve the operational resilience of the individual institutions and thus contribute to strengthening the operational resilience of the Swiss financial market as a whole.

Institutions should therefore continue to focus on activities to ensure operational resilience with a preventive character and suitable measures that enable the development of an operating model with a continuous improvement process in order to operate critical functions in a resilient manner (resilience by design).

At the same time, FINMA will continue and intensify its institution-specific supervisory activities to ensure operational resilience. In particular, there are plans to conduct scenario analyses in greater depth and to create the conditions for sector-wide testing in the long term. FINMA is also monitoring international developments such as those of the IAIS,[22] and examining whether it would be appropriate to extend the supervisory requirements for ensuring operational resilience to other institutions supervised by FINMA.

[20] Not all *Horizontal Reviews of Operational Resilience 2025* have been concluded as at the date of publication of this guidance.

[21] See margin nos. 102 and 113, FINMA Circ. 23/1.

[22] IAIS refers to the International Association of Insurance Supervisors.