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

Circular 2023/1
Operational risks and resilience – banks

Managing operational risks and ensuring operational resilience

Reference:	FINMA Circ. 23/1 “Operational risks and resilience – banks”
Date:	7 December 2022
Entry into force:	1 January 2024
Concordance:	former FINMA Circ. 08/21 “Operational risk – banks”, dated 20 November 2008
Legal framework:	FINMASA Articles 7 para. 1 let. b and 29 para. 1 BA Article 1*b* para. 3 let. b, Articles 3 para. 2 let. a and 3f BO Articles 12 and 14*e* FinIA Articles 9 and 49 FinIO Articles 12 and 68
Annex 1:	Explanatory graphic for operational resilience

Adressees																																			
BankA				**ISA**			**FinIA**						**FinMIA**						**CISA**						**AMLA**		**Other**									
Banks	Financial groups and congl.	Persons under Article 1*b* BA	Other intermediaries	Insurers	Insurance groups and congl.	Intermediaries	Portfolio managers	Trustees	Managers of collective assets	Fund management companies	Investment firms (proprietarian trading)	Investment firms (non propriet. trading)	Trading venues	Central counterparties	Central securities depositories	Trade repositories	Payment systems	Participants	SICAVs	Limited partnerships for CISs	SICAFs	Custodian banks	Representatives of foreign CISs	Other intermediaries	SRO	SRO-supervised institutions	Audit firms	Rating agencies							
X	X	X									X	X																							

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

Index

I. Subject and scope of application

This Circular relates to the rules on the segregation of duties, risk management and internal controls contained in the Banking Ordinance (Arts. 12 and 14*e* BO, SR 952.02) and the Financial Institutions Ordinance (Arts. 12 and 68 FinIO; SR 954.11) and sets out the corresponding supervisory practice. It takes account of the Basel Committee's principles for the sound management of operational risk[1] and operational resilience[2]. 1

This Circular applies to banks under Article 1*a* and persons under Article 1*b* of the Banking Act (BA; SR 952.0), securities dealers under Article 2 para. 1 let. e and Article 41 of the Financial Institutions Act (FinIA; SR 954.1), and financial groups and financial conglomerates under Article 3*c* BA and Article 49 FinIA. In the following, banks, persons under Article 1*b* BA, securities firms, financial groups and financial conglomerates are referred to collectively as "institutions". 2

II. Definition of terms

Operational risk is defined in Article 89 CAO. It refers to the risk of financial loss resulting from inadequate or failed internal processes or systems, inappropriate actions taken by people or mistakes made by them, or from external events. This includes the financial losses that can result from legal or compliance risks. Operational risk management typically also takes other types of damage into account[3], provided that these can ultimately also result in financial loss. It does not include strategic risk. 3

Inherent risks are operational risks that the institution is exposed to through its products, activities, processes and systems, without taking control or mitigation measures into account. 4

Residual risks are operational risks that the institution is exposed to after taking control and mitigation measures into account. 5

Information and communication technology (ICT) refers to the physical and logical (electronic) architecture of IT and communication systems, the individual hardware and software assets, networks, data and operating environments. 6

Critical data are data that, in view of the institution's size, complexity, structure, risk profile and business model, are of such crucial significance that they require increased security measures. These are data that are crucial for the successful and sustainable provision of the institution's services or for regulatory purposes. When assessing and determining the criticality of data, the confidentiality as well as the integrity and availability must be taken into account. Each of these three aspects can determine whether data is classified as critical. 7

Critical processes are processes whose significant disruption endanger the provision of critical functions. They are part of the critical functions. 8

[1] BCBS Revisions to the Principles for the Sound Management of Operational Risk (31 March 2021).

[2] BCBS Principles for Operational Resilience (31 March 2021).

[3] For example, negative impact on reputation, possible loss of confidence and loss of clients, negative impact on the market, negative regulatory impact (e.g. possible loss of licence).

Business continuity management (BCM) refers to the institution-wide approach for recovering the operation of critical processes in the event of a significant disruption going beyond incident management. It defines the response to significant disruptions. Effective BCM reduces the residual risks in connection with significant disruptions. 9

The *recovery time objective (RTO)* is the time within which an application, system and/or process must be recovered. The *recovery point objective (RPO)* is the maximum tolerable period during which data is lost. 10

The *business continuity plan (BCP)* is a forward-looking plan that sets out the necessary procedures, recovery options and alternative resources (the recovery processes) for ensuring continuity and recovering critical processes. 11

The *disaster recovery plan (DRP)* defines the recovery processes for achieving the recovery goals in the event of a catastrophic failure or destruction of the ICT and taking into account the possible loss of key personnel. 12

Crisis situations are exceptional situations that potentially threaten the institution's existence, and that cannot be managed with ordinary measures and decision-making authority. They differ from incidents and significant disruptions that can be overcome with incident management in normal operation or with the defined BCPs and DRPs. 13

Critical functions include: 14

a. the activities, processes and services – including the underlying resources necessary for their provision – whose disruption would jeopardise the institution's continuation or its role on the financial market and thus the proper functioning of the financial markets; and 15

b. the systemically important functions under Article 8 BA. 16

The *tolerance for disruption* is the extent (e.g. the duration or expected damage) of the disruption of a critical function that the institution is willing to accept, taking severe but plausible scenarios into account. A tolerance for disruption must be defined for each critical function. 17

Operational resilience refers to the institution's ability to restore its critical functions in case of a disruption within the tolerance for disruption. That is to say, 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 learn from them, so as to minimise the impact of disruptions on the provision of critical functions. An operationally resilient institution has designed its operating model in such a way[4] that it is less exposed to the risk of disruptions in relation to its critical functions. Operational resilience thus reduces not only the residual risks of disruptions, but also the inherent risk of disruptions occurring. Effective operational risk management helps strengthen the institution's operational resilience. 18

[4] Often also called *resilience by design*.

III. Principle of proportionality

This Circular applies to all addressees. However, the requirements are to be implemented on a case-by-case basis, depending on the size, complexity, structure and risk profile of each institution. FINMA can relax or tighten the rules in individual cases. 19

Banks and securities firms in FINMA Categories 4 and 5 are exempt from complying with margin nos. 33–38, 41–46, 48, 51, 57, 73, 74, 76–78, 80, 87, 92, 93, 96, 103, 104 and 110–112. 20

Institutions under Articles 47*a*–47*e* CAO, persons under Article 1*b* BA, and investment firms (non-proprietarian trading) are also exempt from complying with margin nos. 72, 75, 79 and 105–109. 21

IV. Operational risk management

A. Overarching operational risk management

Operational risk management forms part of institution-wide risk management under FINMA Circular 2017/1 "*Corporate governance – banks*". 22

The board of directors approves the basic principles for the management of operational risks relevant for the institution and monitors their application. Among others, these include the ICT risks, the cyber risks, the risks relating to critical data, the risks resulting from the design and implementation of BCM and, where applicable, the risks from cross-border service business. At least once a year, the board of directors approves the risk tolerance for operational risk in accordance with the risk policy, taking the institution's strategic and financial goals into account. In doing so it considers the results from the risk and control assessments under margin no. 30. It accepts either the extent to which the institution is exposed to operational risk, or decides to adjust the risk tolerance and make the strategic changes necessary for this[5]. 23

The board of directors regularly approves strategies for dealing with ICT, cyber risks, critical data and BCM, and monitors their application. 24

The executive board ensures in a comprehensible way that the operational risks are identified, assessed, limited and monitored, and that the effectiveness of both the design and also of the implementation of this operational risk management is regularly reviewed. It takes risk-specific supplementary or intensified measures in order to limit the inherent risks deemed to be material[6] as the situation demands. 25

To raise awareness among employees for reducing relevant operational risks, particularly ICT risks, cyber risks, risks with regard to critical data and the risks resulting from the 26

[5] For example, a change to the business model.

[6] Often called top risks or key risks.

design and implementation of BCM, measures are to be implemented and carried out taking into account their tasks, competencies and responsibilities[7].

If necessary, FINMA will define more stringent requirements for operational risk management for specific topics as part of ongoing supervision. This will be done cautiously and in accordance with the proportionality principle. 27

The operational risks must be categorised in a uniform manner across the institution and listed in an inventory. The categorisation may be performed based on the categorisation of event types used to calculate the minimum capital requirements for operational risk or based on an internal taxonomy. The categorisation must be applied consistently in all areas of the institution and in all components of operational risk management. 28

Internal[8] and external[9] factors shall be taken into account for identifying operational risks. The identified operational risks shall be assessed in a comprehensible way both from the perspective of inherent as well as residual risks. 29

The identification and assessment of operational risks shall be based on at least review results[10] and regularly conducted risk and control assessments. The risk and control assessments shall take into account the inherent risks, the effectiveness of the existing control and mitigation measures and the residual risks. 30

To assess the existing control and mitigation measures, in particular a regular assessment of the effectiveness of key controls must be performed and documented by an independent control body (design effectiveness and operating effectiveness testing). Key controls are those control and mitigation measures that minimise the inherent risks deemed to be material. The separation of tasks, competencies and responsibilities to ensure independence and prevent conflicts of interests shall also be regularly assessed. 31

Ad hoc risk and control assessments shall be conducted prior to major changes in products, activities, processes and systems. These shall take into account the operational risks associated with the change process and the operational risks of the target state. If necessary, the risk tolerance should be adjusted and control and mitigation measures implemented. 32

Depending on the type, scope, complexity and risk of institution-specific products, activities, processes and systems, the following tools and methods shall be applied: 33

a. Systematic collection and analysis of internal loss data and relevant external events associated with operational risk; 34

b. Risk and control indicators for monitoring operational risk and identifying relevant risk increases in a timely manner; 35

[7] Among other things, this includes carefully selecting employees, ensuring that they are suitably qualified for their tasks, competencies and responsibilities and providing them with continuing education within the context of their activities.

[8] Internal factors include, for example, changes to products, activities, processes and systems, review results and internal losses resulting from operational risks.

[9] External factors include, for example, loss events at other institutions, changes in the security situation (e.g. as a result of environmental influences, cyber attacks or terrorism) or changes to the regulatory requirements.

[10] Review results encompass here results of internal and external audits, where available, as well as results of reviews performed, for example, by the business and organisational areas, the risk control and compliance functions or supervisory authorities.

c. Scenario analyses and/or estimates of the loss potential in view of or in comparison with the minimum capital requirements for operational risk; 36

d. Comparative analyses (read-across), for example, analyses of the relevance of review results for other areas of the institution or comparisons between the results of the risk and control assessments for various areas. 37

The risk tolerance for operational risk takes account of both the tolerance in relation to inherent[11] as well as residual operational risk and is monitored using risk or control indicators. 38

The risk control function reports to the board of directors at least annually and to the executive board at least every six months in accordance with margin nos. 75–76 of FINMA Circ. 17/1 on the operational risks at the top level[12] of the categorisation defined in accordance with margin no. 28, on their comparison with the defined risk tolerance, and on details of material internal losses. 39

In relation to the relevant ICT and cyber risks, the report for the executive board produced at least annually shall also contain information on the development of these risks, on the effectiveness of the corresponding key controls, and on material internal and external events in connection with these risks. 40

The internal reporting in accordance with margin no. 39 shall contain in addition the following information: 41

- relevant, external factors in accordance with footnote 9, 42
- summary overview of the effectiveness of the key controls in accordance with margin no. 31, 43
- emerging operational risks; 44
- results from the application of additional tools and methods in accordance with margin no. 33. 45

In accordance with the principle of proportionality, for systemically important banks, regular reporting on operational risks shall also be conducted at the level of the business or organisational areas that are exposed to relevant or material operational risks. 46

B. ICT risk management

a) ICT strategy and governance

The basic expectations for the strategy, governance and raising of awareness in relation to ICT are set out in margin nos. 23–26 and 40. 47

ICT risk management shall take into account relevant internationally recognised standards and practices as well as the influence of new technological developments on 48

[11] The risk tolerance in relation to inherent risk takes account of strategic decisions in relation to the business or operating model, for example, tolerance for the inherent risks associated with serving certain client segments or countries, with offering certain products, with using primarily manual processes, with relying on a complex IT infrastructure or with outsourcing certain operations.

[12] The top level of the categorisation is often referred to as level 1. The reporting can also take place on a more detailed level.

the ICT risks.

The executive board shall ensure that procedures, processes and controls as well as tasks, competencies and responsibilities are implemented and documented both for change management and for ICT operations (run, maintenance). These shall be adequately resourced with qualified staff. 49

b) Change management

Change management shall define the procedures, processes and controls for all phases in the development or procurement of ICT. In each of these phases it shall consider the impact of the change on the ICT risks. It shall focus in particular on the requirements with regard to confidentiality, integrity and availability. 50

It must be ensured that the development or test environments are separate from the ICT production environment. This also involves the clear allocation of tasks, competencies and responsibilities and laying down rules for the associated access rights. 51

When developing and procuring ICT, functional and non-functional requirements[13] shall be clearly defined and approved; they shall be tested and validated based on their criticality. 52

c) ICT operations (run, maintenance)

The institution shall keep one or more inventories of the ICT assets. The inventory shall include hardware and software assets as well as the storage locations of critical data. Both dependencies within the institution as well as interfaces to significant external service providers should be taken into account. 53

The inventory is available in real time and shall be reviewed and updated regularly with regard to its completeness and accuracy. 54

The institution shall have procedures, processes and controls in place that ensure the confidentiality, integrity and availability of the ICT production environment, taking into account the respective risk tolerance. 55

The institution shall ensure that it can transition smoothly to its BCP and DRP processes in the event of significant disruptions to its ICT operations. It shall implement adequate back-up processes and recovery processes that are tested and validated regularly. 56

The institution shall have procedures, processes and controls in place to ensure that ICT that its nearing the end of its operational life or whose planned decommissioning date has passed is dealt with in a risk-oriented way. 57

d) Incident management

The institution shall have procedures, processes and controls in place for dealing with significant ICT incidents, including those resulting from dependencies on external service providers and outsourcing operations within the group. In this regard, the full life-cycle of significant ICT incidents must be taken into account and tasks, competencies and responsibilities for dealing with these incidents must be defined. 58

[13] E.g. with regard to architecture or information security requirements.

Dealing with significant ICT incidents must be coordinated and linked with the processes for BCM and the DRP. 59

ICT incidents that are regarded by the institution as a significant disruption in the provision of its critical processes and are of material significance for supervision must be reported to FINMA without delay. 60

C. Cyber risk management

The basic expectations for the strategy, governance and raising of awareness in relation to cyber risks are set out in margin nos. 23–26 and 40. 61

The institution shall define clear tasks, competencies and responsibilities. It must cover at least the following aspects in accordance with internationally recognised standards and practices, and ensure their effective implementation through appropriate procedures, processes and controls and continuously develop and improve them: 62

a. Identification of the institution-specific threat landscape from cyber attacks[14] and assessment of the possible impacts of exploiting vulnerabilities with regard to the inventoried ICT assets and the electronic critical data (in accordance with margin nos. 53, 54 and 7); 63

b. Protection of the inventoried ICT assets and the electronic critical data from cyber attacks by implementing appropriate protective measures, particularly with regard to the confidentiality, integrity and availability; 64

c. Timely logging and detection of cyber attacks on the basis of a process for the systematic and consistent monitoring of the inventoried ICT assets and the electronic critical data; 65

d. Response to identified vulnerabilities and cyber attacks by developing and implementing appropriate processes for taking rapid containment and remediation measures; and 66

e. Ensuring the prompt recovery of normal business operations after a cyber attack through appropriate measures. 67

Cyber risk management must ensure that a successful or partially successful cyber attack is analysed based on its materiality for critical inventoried ICT assets or electronic critical data and critical processes (including outsourced services and functions) and that the reporting obligation under the FINMASA is met. After an initial assessment and preliminary notification to the body responsible at FINMA within 24 hours, the report in accordance with the catalogue of requirements on the EHP survey and application platform (mandatory fields) must be submitted to FINMA within 72 hours. Once the institution has finished processing the case, a conclusive root cause analysis corresponding to the degree of severity must be submitted to the body responsible at FINMA. 68

[14] Attacks on the confidentiality, integrity and availability of ICT as well as the electronic critical data that take place as a result of external or internal attackers exploiting vulnerabilities or circumventing protective measures.

The executive board shall arrange for vulnerability assessments[15] and penetration tests[16] to be conducted regularly. These must be performed by qualified staff with adequate resources. All inventoried ICT assets that are accessible over the internet must be taken into account. In addition, inventoried ICT assets that are not accessible over the internet, but that are necessary for the provision of critical processes, or that contain electronic critical data, must be included as well. 69

Risk-based, threat intelligence-related scenario cyber exercises[17] must be conducted on the basis of the institution-specific threat landscape. The result of the exercises must be documented and reported in an appropriate form. 70

D. Critical data risk management

The basic expectations for the strategy, governance and raising of awareness in relation to the risks of critical data are set out in margin nos. 23–26. 71

The executive board shall define appropriate processes, procedures and controls as well as clear tasks, competencies and responsibilities for dealing with the data identified as critical by the institution. Furthermore, the executive board shall appoint a unit to establish the framework for ensuring the confidentiality, integrity and availability of critical data and to monitor its observance. 72

The institution shall identify its critical data in a systematic and comprehensive way, categorise it on the basis of its criticality and define clear responsibilities. 73

The critical data defined by the institution must be managed throughout its entire life-cycle. 74

In the management of critical data, in particular the confidentiality, integrity and availability of the critical data must be ensured through appropriate processes, procedures and controls. 75

Critical data must be adequately protected from being accessed and used by unauthorised persons during operations and during the development, change and migration of ICT. This also applies to critical data in test environments. 76

The ICT assets that store or process critical data must be afforded particular protection. Access to these data must be regulated systematically and monitored continuously. 77

Access to critical data and processing functionalities shall be restricted to persons who require this to carry out their tasks[18]. The institution must have an authorisation system in place. Access to this authorisation system must be afforded particular protection and reviewed on a regular basis. The authorisations included in the authorisation system must be reviewed on a regular basis. 78

[15] Analysis used to identify existing software vulnerabilities and security gaps in the IT infrastructure towards cyber attacks.

[16] Targeted audit and exploitation of software vulnerabilities and security gaps in the ICT.

[17] Taking into account margin no. 19, such cyber exercises may include, for example, tabletop, red team exercises etc.

[18] For example, need-to-know and least privilege principles.

If critical data is stored outside of Switzerland[19] or if it can be accessed from abroad, increased risks associated with this must be adequately mitigated and monitored via suitable means and the data afforded particular protection. 79

Both internal and external persons who can access critical data or who can change these must be selected carefully. These persons must be monitored with the help of appropriate measures[20] and given regular training in the handling of these data. Increased security requirements shall apply to persons with increased privileges[21]. In addition, a list of all persons with privileged access rights must be kept and updated on a regular basis. 80

Incidents that substantially impair the confidentiality, integrity or availability of critical data must be reported to FINMA without delay. 81

When selecting service providers that can process[22] or view critical data, due diligence must be particularly thorough. Clear criteria for assessing how service providers handle critical data must be defined and checked before entering into a contractual agreement. The service providers must be monitored and checked periodically as part of the institution's internal control system. 82

E. Business continuity management (BCM)

The basic expectations for the strategy, governance and raising of awareness in relation to risks resulting from the design and implementation of BCM are set out in margin nos. 23–26. 83

Every relevant business and organisational area must identify its critical processes and the resources required for these[23] in a business impact analysis (BIA). 84

The institution shall define the RTO and RPO for the critical processes in accordance with margin no. 10. These shall be coordinated with the necessary service providers[24] and adherence to the RTO and RPO shall be regulated by service level agreements or contracts or by other appropriate procedures, processes and controls. 85

The institution shall define at least one BCP in accordance with margin no. 11 that also describes the conditions triggering the plan and the decision-making processes, and takes into account the loss of resources in accordance with margin no. 84. The acceptance of residual risks must be adequately documented. 86

The BIA and BCP shall be prepared and documented in a consistent manner following institution-wide guidelines. They must be reviewed and updated annually and on an ad hoc basis in the event of significant changes to the business operations (reorganisations, development of a new business segment etc.). 87

[19] For example, in the context of cloud or hosting solutions.

[20] For example, analysis of log files, "four eyes principle" etc.

[21] For example, persons with administrator rights, users with functional access to a large quantity of critical data etc.

[22] Processing: any handling of critical data, irrespective of the means and procedures used, in particular the collection, saving, storage, use, changing, disclosing, archiving, deletion or destruction of data.

[23] Staff, facilities (e.g. building, workplace infrastructure), information, IT systems or IT infrastructure (including communication systems), dependencies on other areas of the institution and on third parties, e.g. external service providers and suppliers (outsourcing), central banks or clearing houses.

[24] For example, with the IT department, other units of the institution or external parties.

The institution shall define at least one DRP as part of the BCP. If critical processes or parts thereof are outsourced, the DRP shall take into account the external dependencies and contractual provisions as well as alternative solutions. The DRP must be reviewed and updated on an ad hoc basis in the event of significant changes and at least annually. 88

In crisis situations, a crisis unit shall take on the task of crisis management until order is restored. The conditions triggering a crisis and the tasks, competencies and responsibilities of the crisis unit must be regulated in advance and the crisis organisation aligned to the business activities and geographical structure of the institution. The availability of responsible persons in crisis situations must be ensured. 89

The institution shall define a communication strategy for internal and external communication in crisis situations. 90

The implementation of the BCP and DRP as well as the functioning of the crisis organisation must be regularly evaluated through tests. Systematic plans shall be drawn up for this, which ensure regular coverage. Various means of testing of varying intensity and effectiveness can be selected including, for example, tabletop exercises. 91

The most important measures according to the BCP and DRP and the crisis organisation must be tested at least once a year. 92

Relevant stakeholder groups, including those in specialist and IT functions, shall take part in the tests in order to familiarise themselves with the recovery processes. 93

The tests shall encompass various severe but plausible scenarios and take into account recovery dependencies, including those that exist with internal or external third parties. 94

Regular reporting to the board of directors and the executive board shall include information about the testing and review activities carried out and their results. It shall clearly show prioritisations made (e.g. prioritisation of the critical processes necessary for the provision of the critical functions in accordance with margin no. 14) and recognised gaps in the coverage of other critical processes. 95

The employees and members of the crisis organisation shall be adequately trained in their tasks, competencies and responsibilities resulting from the various BCM activities, both when new employees join the institution and as part of regular training. 96

F. Management of risks from cross-border service business

If institutions or their group companies provide services or distribute financial products cross-border, then the risks resulting from the application of foreign legislation (tax, criminal, anti-money laundering legislation etc.) must also be adequately identified, limited and controlled. 97

The institutions shall conduct a thorough analysis of their cross-border service business and cross-border distribution of financial products, examining the legal framework and associated risks. Based on this analysis, the institutions shall take the necessary strategic and organisational measures to eliminate and minimise risk, and continuously adapt these to changing conditions. In particular, they shall have the necessary country-specific specialist knowledge, define specific service models for the countries served, train employees and ensure compliance with the guidelines through appropriate organisational measures, directives, remuneration and sanctions models. 98

The risks generated by external asset managers, intermediaries and other service providers must also be taken into account. Accordingly, a diligent approach must be adopted in selecting and instructing these partners. 99

This basic approach also covers situations where a foreign-based subsidiary, branch or similar serves clients of a Swiss financial institution cross-border. 100

V. Ensuring operational resilience

The institution shall identify its critical functions and their tolerances for disruption. These must be approved by the board of directors. The board of directors must also regularly approve and monitor the approach for ensuring operational resilience. 101

The institution shall take measures to ensure operational resilience, taking into account severe but plausible scenarios[25]. 102

The critical functions and the associated tolerances for disruption according to margin no. 14 must be approved at least annually by the board of directors. 103

The institution shall coordinate the relevant components of a comprehensive risk management framework, such as operational risk management, including ICT and cyber risk management, business continuity management, outsourcing management (cf. FINMA Circular 2018/3 “Outsourcing”), and emergency planning (Chapter VI.) such that these contribute to strengthening the institution’s operational resilience. This includes an appropriate exchange of relevant information between these various areas. 104

Reporting to the board of directors and the executive board must take place annually and in the event of significant control weaknesses or incidents that jeopardise operational resilience. 105

Internal and external threats and the corresponding exploitation of vulnerabilities shall be identified and assessed for the critical functions. The resulting operational risks shall be identified, assessed, limited and monitored as part of operational risk management. 106

The institution shall keep an inventory of its critical functions, which is reviewed and updated at least annually. This inventory shall contain the tolerances for disruption of the critical functions, as well as connections and dependencies between the necessary critical processes and their resources[26] for providing the critical functions. 107

As a minimum, the significant operational risks and the key controls must be documented for the critical functions. 108

The critical functions and the critical processes and resources required for these shall be covered by BCPs pursuant to Chapter IV./E. 109

The ability to provide critical functions within their tolerance for disruption in severe but plausible scenarios shall be tested or exercised regularly. These also include scenarios that differ from shorter and more limited interruptions and that are characterised by a 110

[25] It cannot be ruled out that some scenarios cannot be managed without state involvement (e.g. pandemics, wars, long-term power shortages). For such scenarios, preliminary work must be carried out by the institution for the purpose of strengthening its operational resilience to these scenarios in so far as its means allow.

[26] Including the ICT assets of the inventory in accordance with margin no. 53 relevant to the critical functions.

longer duration (e.g. over several months) and a lack of basic resources[27]. The tests or exercises must be designed in such a way that they do not fundamentally endanger the institution.

For systemically important banks, the BCP, DRP and the crisis organisation in accordance with Chapter IV./E. that are relevant for the continuation of the critical functions in accordance with margin no. 14 must be coordinated with the emergency planning in accordance with Chapter VI. 111

VI. Continuation of critical services during the resolution and recovery of systemically important banks

As part of their emergency planning, systemically important banks shall take the necessary measures for the uninterrupted continuation of systemically important functions (Art. 9 para. 2 let. d BA in conjunction with Art. 60 ff. BO). They shall identify the services necessary to continue the systemically important functions in the event of resolution, recovery or restructuring ("critical services") and take the measures necessary for their continuation. In doing so they shall take into account the requirements issued by international standard setters in this context. 112

VII. Transitional provisions

A. Concerning ensuring operational resilience

The identification of critical functions, the definition of tolerances for disruption and initial approvals in accordance with margin nos. 101 and 103, as well as initial reporting in accordance with margin no. 105, will be expected following the Circular's entry into force. A transitional period of one year from the entry into force shall apply for fulfilling the requirements in accordance with margin nos. 106–109 and the first tests in accordance with margin no. 110. It is expected that operational resilience will be ensured in accordance with margin no. 102 and the requirements met in accordance with margin nos. 104 and 111 within a transitional period of two years. 113

B. Concerning the capital requirements for operational risk

The capital requirements for operational risk in accordance with Article 89 ff. CAO shall be based on margin nos. 3–116 of FINMA Circular 2008/21 "Operational risk – banks" until the entry into force of the CAO revised as part of the final Basel III revision package and the implementing FINMA ordinance. 114

[27] Examples include a pandemic, a power shortage, a prolonged downtime resulting from the insolvency of a key service provider (as an example of a stressed exit by a service provider) or a long-term prohibition of foreign governments, according to which foreign-based cloud providers or other service providers are no longer permitted to serve Swiss firms.

Annex 1

Explanatory graphic for operational resilience

Components for the provision of critical functions