

# FINMA's update of the Operational Risk Circular: information and communication technology (ICT), data management and operational resilience in focus



DE

EN

With the full revision of the 'Operational Risk – Banks' circular 2008/21, FINMA refines its supervisory practice regarding the management of operational risks. The areas information and communication technology (ICT), dealing with critical data, and cyber risks are materially changed. The to-be-approved circular will newly also cover requirements to operational resilience.

The new circular on operational risk and operational resilience will become effective on 1 January 2024 with expected transitional periods.

## What are the key changes?

- Incorporation of operational resilience, extending on previous regulatory standards for business continuity management (BCM).<sup>1</sup>
- Alignment with other regulatory provisions<sup>2</sup> in the areas of digitalisation and ICT, cyber risks, and dealing with critical data.
- Refinement but no significant changes to existing provisions on the management of operational risks.

## What are the new principles?

The new circular contains eight principles. Seven of them directly evolve from the previous principles and/or other sources of regulatory requirements already in effect. One of the eight principles, operational resilience, is new (see illustration 1).<sup>3</sup>









Circular principles	
Management of operational risks	<b>Overarching operational risk management</b>  Principle A is an evolution from the former first three principles of FINMA-Circ. 2008/21. It aims at clarifying possible misinterpretations. There are no major changes in substance.
	<b>ICT risk management</b>  Principle B is linked to the <b>former principle on IT infrastructure</b> . It specifies the regulatory requirements described in the revisions to the 'Principles for the Sound Management of Operational Risk' Basel Committee on Banking Supervision's (BCBS) paper.
	<b>Cyber risk management</b>  The provisions on the management of cyber risks are extended within Principle C. The new circular formally introduces <b>scenario based cyber exercises</b> and <b>integrates the existing regulatory reporting requirements</b> on cyber attacks.
	<b>Critical data risk management</b>  Principle D expands the qualitative requirements described in the BCBS papers, now including any type of data that are perceived as critical regarding its confidentiality, integrity and availability ( <b>moving away from only electronic customer data</b> ).
	<b>Business continuity management (BCM)</b>  Principle E is a refinement of the principle-based, self-regulatory guidelines and recommendations issued by the Swiss Banking Association regarding BCM. There are no additional requirements or significant adjustments.
	<b>Management of risks from cross-border services</b>  Principle F shows no change to previous qualitative requirements on the management of risks arising from cross-border services. Only the terminology 'financial services' was changed to 'services'. <b>This principle is not covered by our presentation.</b>
<b>new</b>	
Ensuring operational resilience	 <b>New principle in the circular based on the 'Principles for Operational Resilience' issued by BCBS, aligned with international standards.</b>
Continuation of critical services during the resolution and recovery of systemically important banks	 This principle remains unchanged. Only linguistic adjustments were implemented. <b>This principle is not covered by our presentation.</b>

Illustration 1: Overview of new principles and their changes

<sup>1</sup> 'Recommendations for Business Continuity Management' by the Swiss Banking Association.

<sup>2</sup> 'Principles of Operational Resilience' (POR) and the revised 'Principles of the Sound Management of Operational Risk' (PSMOR) by the Basel Committee on Banking Supervision (BSBS).

<sup>3</sup> Delimitation: The capital requirements will no longer be a subject of the circular on operational risk and will instead be included in the to-be-revised Capital Adequacy Ordinance and the associated FINMA implementing provisions. The fully revised Operational Risk and Operational Resilience circular will result in changes to FINMA circular 2013/3 'Auditing', which will undergo a partial revision at the same time. It's also scheduled to become effective on 1 January 2024.

Below, we summarise selected changes for the board of directors, executive committee and risk control.<sup>4</sup>

## What changes for the board of directors (BoD)?

ICT, cyber and critical data risk management	<ul style="list-style-type: none"> <li>• Approve and supervise the ICT strategy as well as the management of ICT risks and give assurance of the confidentiality, integrity and availability of the ICT (Mn 23-24, 47);</li> <li>• Follow international standards regarding the management of ICT risks and consider the influence of new technologies on the ICT risks (Mn 48)<sup>4</sup>;</li> <li>• Approve and supervise the cyber risks strategy as well as the management of cyber risks (Mn 23-24, 61);</li> <li>• Consider international standards and best practices regarding the management of cyber risks (Mn 62-67).</li> <li>• Approve and supervise the protection of critical data such as the establishment of a data strategy including a governance and organisation framework, processes, data and information architecture as well as data security (Mn 23-25, 71).</li> </ul>	<b>Operational resilience's aspects</b>
BCM and operational resilience	<ul style="list-style-type: none"> <li>• Approve and supervise the BCM strategy and governance (Mn 23-25, 83) and the operational resilience strategy and approach (Mn 101,104)<sup>4</sup> (also see text box to the right);</li> <li>• Fully engage in times of crisis situations to supervise the ability to continue critical processes and the achievement of key business targets. Agree on an action plan for such incidents (Mn 89-90).</li> <li>• Approve critical functions and their disruption tolerance annually and be ware about the impact on the unavailability of critical functions (Mn 103, 105, 106)<sup>4</sup>.</li> </ul>	<div style="background-color: #34495e; color: white; padding: 5px; margin-bottom: 5px;">1 BCM with focus on recovering after a disruption</div> <div style="background-color: #34495e; color: white; padding: 5px; margin-bottom: 5px;">2 Strategic dimension: identification of critical functions top-down</div> <div style="background-color: #34495e; color: white; padding: 5px;">3 Preventive dimension: resilience by design i.a. preventive measures and continuous learning and improvement</div>

## What changes for the executive committee (EC)?

ICT, cyber and critical data risk management	<ul style="list-style-type: none"> <li>• Implement supervision in the area of the ICT strategy, the management of ICT risks as well as the assurance of the confidentiality, integrity and availability of the ICT as defined by the BoD (Mn 25);</li> <li>• Ensure that rules, processes and controls for (i) change management and (ii) ITC operations (run/maintenance) are defined and implemented (Mn. 49, 55, 57)<sup>4</sup>;</li> <li>• Ensure adequate qualification of resources staff (Mn 49).</li> <li>• Implement the strategy regarding the management of cyber risks as defined by the BoD (Mn 25);</li> <li>• Define clear tasks, competencies and responsibilities and ensure effective implementation of international standards (Mn 62-67);</li> <li>• Ensure that cyber risk analysis is performed on institution-specific potential threats as well as give mandate on weakness analysis and penetration tests (Mn 69-70).</li> <li>• Manage the protection of critical data through its entire life cycle (incl. data ownership, data storage, retention and deletion) as well as the definition of sufficient processes, procedures and controls including clear tasks, roles and responsibilities (Mn 25, 72, 74-75)<sup>4</sup>.</li> </ul>
BCM and operational resilience	<ul style="list-style-type: none"> <li>• Set up the BCM strategy and define supplementary measures (if required) (Mn 25, 83);</li> <li>• Define crisis organisation (incl. trigger, crisis unit, communication strategies (Mn 25, 83, 89-90);</li> <li>• Fully engaged in the continuation of critical processes and achievement of key business targets during crisis situations. This includes having an agreed action plan defined on how to react prior to the event (Mn 89-90).</li> <li>• Assure adequate mitigation actions are implemented to adhere to the defined disruption tolerances (Mn 101-105)<sup>4</sup>;</li> <li>• Be informed about the impact on the unavailability of critical functions and the (multiple) interruption tolerances for all the critical functions (Mn 105).</li> </ul>

<sup>4</sup> FINMA categories 4 and 5 are not affected by all these changes. FINMA may order reliefs or further restrictions in individual cases.

## What changes for risk control (RC)?

### ICT, cyber and critical data risk management

- Raise awareness of employees (Mn 26);
- Set rules for the change management process and controls such as impact assessment of change requests; adequate governance structure; separation between ICT environments for development/testing and production (incl. access rights); rules for ICT procurements (incl. definition of requirements) (Mn 50-52)<sup>4</sup>;
- Set up and review regularly an inventory of the ICT assets (Mn 53-54);
- Implement back up and recovery processes and test them regularly (Mn 56);
- Implement dedicated processes and controls to deal with ICT incidents (incl. FINMA notification and consideration of the incident lifecycle) (Mn 58-60);
- Ensure that every (partially) successful cyber attack is analysed and the reporting obligations under FINMASA are met (Mn 68);
- Perform regular vulnerability assessments and penetration tests and institute-specific scenario-based exercises (incl. at least ICT systems required for the provision of critical functions or those that contain critical data or can be assessed via Internet) (Mn 69-70);
- Cyber risk management (identification, assessment, mitigation and monitoring) is included in operational risk management and documented in a comprehensible manner. RC submits a report to the ExB at least annually on the development of the threat and risk profile, any damage on the back of cyber attacks as well as key control's effectiveness (Mn 40).
- Raise awareness, monitor and list employees with access to critical data (Mn 26, 80)<sup>4</sup>;
- Identify and categorise the critical data (Mn 73)<sup>4</sup>;
- Define data responsibilities and access rights (Mn 73, 76-78)<sup>4</sup>;
- In case of critical data is stored abroad or can be assessed from abroad additional risk mitigation and monitoring measures should be implemented (Mn 79);
- Due diligence and monitoring of employees and service providers who can assess critical data (Mn 80, 82);
- Create and keep up-to-date a list with persons with privileged access rights (Mn 80)<sup>4</sup>.

### BCM and operational resilience

- Raise awareness of employees (focus on crisis organisation) (Mn 26, 96)<sup>4</sup>;
- Every business area should conduct a business impact analysis (BIA) to identify the critical processes and required resources as well as define objectives (Mn 10, 84-85);
- Define at least one business continuity plan (BCP) and one Disaster Recovery Plan (DRP) (Mn 86, 88,109);
- Annual and ad hoc review of BCP, BIA and DPR (Mn 87,88)<sup>4</sup>;
- Conduct regular tests regarding BCP, DRP and the crisis organisation focusing on severe but plausible scenarios (Mn 91-94)<sup>4</sup>;
- Implement regular reporting to BoD and ExB (Mn 95).
- Identify critical functions and their disruption tolerance and manage the defined measures to ensure operational resilience (Mn 101-102);
- Maintain an up-to-date inventory of critical functions (Mn 107);
- Keep record of key controls and operational risks related to the critical functions (Mn 108);
- Establish a testing framework (e.g. Walk-Through or Table Top-Tests) to regularly review the ability to perform critical functions at times of operational disruption within their interruption tolerances (Mn 110)<sup>4</sup>;
- Annual and ad hoc reporting to BoD and ExB (Mn 105).

**Start now using the time to prepare and to secure budgets that will be required for the significant changes.**

Are you interested to discuss how we can support you in becoming compliant with the new circular?



**Salome Forrer**  
Risk Consulting  
[salome.forrer@pwc.ch](mailto:salome.forrer@pwc.ch)



**Vinay Kalia**  
Risk Consulting  
[vinay.kalia@pwc.ch](mailto:vinay.kalia@pwc.ch)