Operational Resilience in Swiss Banking:

When Compliance Meets Confusion

Forensic analysis · SRA forum data 2015–2026 · BCBS–FINMA gap · Six board-level challenges

85%
had NOT conducted any resilience testing

267
Swiss institutions surveyed by FINMA

68%
of SRA OR events focused on cyber only

48h
median tolerance — from IT recovery, not board

Sources: FINMA Guidance 05/2025 (267-institution survey, Nov 2025)
Swiss Risk Association event library 2015–2026 (273 events)

KEY TAKEAWAYS

- Cyber dominance has created a governance blind spot
- Tolerance for disruption ≠ IT recovery time
- 85% of Cat.1–3 banks had not tested resilience

Anwarul Hasan (MBA, PhD)
Founder & CEO · Risk Vizon LLC · Zurich, Switzerland
25+ years · UBS · KPMG · Swiss Re | anwarul.hasan@riskvizon.com

Operational Resilience in Swiss Banking:

When Compliance Meets Confusion

By Anwarul Hasan (MBA, PhD)

Founder & CEO, Risk Vizon LLC · Zurich · June 2026

We are now past the 1 January 2026 deadline. Every Category 1–3 Swiss financial institution is, in theory, required to have achieved full operational resilience framework coordination under FINMA Circular 23/1. Yet FINMA's own survey of 267 institutions — conducted barely a month before the deadline — found that **85% had not conducted any resilience testing**, and only **12–15% had achieved the framework coordination** that was supposed to be mandatory from day one of the new year.

Something has gone wrong. Not with the institutions' intentions. Not with the regulators' ambitions. But with the translation layer between international regulatory standards and Swiss implementation — and with how the industry has understood operational resilience as a discipline.

I have spent the past several months conducting a forensic analysis of two data sources: a decade of Swiss Risk Association (SRA) forum programming — 273 events from 2015 to 2026, classified by theme — and the detailed cross-mapping between BCBS Principles for Operational Resilience (d516, 2021) and FINMA Circular 23/1 (2024). What I found is both illuminating and, frankly, concerning.

One Principle Has Dominated the Conversation — Six Have Been Left Waiting

Operational resilience comprises seven interconnected principles from the Basel Committee: governance and board accountability (P1), the use of operational risk management tools for resilience (P2), business continuity for critical operations (P3), mapping critical functions and dependencies (P4), third-party dependency management (P5), full-lifecycle incident management (P6), and resilient ICT and cyber security (P7).

Of 28 SRA events classified under Operational Resilience over ten years, **19 — roughly 68% — addressed cyber and IT risk.** The annual National Cyber Security Events, the cyber risk quantification series, the threat landscape forums — all valuable, all addressing BCBS P7.

But what about P1 through P6?

Board-level accountability for resilience (P1)? Discussed in governance forums, but almost never framed as an operational resilience accountability distinct from general risk oversight. Critical function mapping with board-approved tolerances for disruption (P3/P4)? Zero dedicated SRA events. End-to-end third-party dependency as a resilience discipline (P5)? Addressed under outsourcing and compliance lenses rather than resilience logic. Full-lifecycle incident management for non-ICT events (P6)? Absent from the programme entirely.

© 2026 Risk Vizon LLC

The Regulator's Dilemma: One Circular, Two Frameworks, Zero Labels

FINMA chose to combine two conceptually distinct BCBS frameworks — the 2011 Principles for Sound Management of Operational Risk (PSMOR) and the 2021 Principles for Operational Resilience — into a single circular. This is administratively elegant. It is conceptually perilous.

ORM under PSMOR uses **prevention and mitigation logic** — it asks what can go wrong, how likely, and what the impact. Operational Resilience uses **continuity and absorption logic** — it explicitly assumes certain failures will occur regardless of controls, and asks whether the institution can absorb disruption and keep critical services running.

> "A 'risk appetite' for operational risk asks: how much loss are we willing to accept? A 'tolerance for disruption' asks: how long can our clients, counterparties, and markets survive without us before systemic harm occurs? These are different questions in different dimensions."

The most visible symptom: institutions are setting their disruption tolerances based on what their systems can recover in (median: 48 hours), rather than on what their clients and markets can tolerate. The board sets the tolerance first — the IT recovery programme is then designed to meet it, not the other way around. This is not a calibration error. It is a **category error.**

The Six Compliance Challenges That Deserve Board Attention

1. You probably have two testing programmes when you should have one

FINMA Circular 23/1 requires BCM testing under §83–96 AND resilience scenario testing under §110–111. These are substantively overlapping. Without integration guidance, most institutions are running them as separate exercises — incurring duplication costs and missing synergies that a unified programme would deliver.

2. Your incident management framework has a significant gap

BCBS OR Resilience P6 covers the full incident lifecycle for **all** disruptive event types. FINMA's implementation (§58–60) covers **only ICT incidents.** A rogue trader, a critical process failure, a pandemic-level staffing disruption — none of these have a structured FINMA-mandated incident response lifecycle.

A Swiss bank can be fully compliant with FINMA Circular 23/1 while having no formal response framework for a rogue trader event. Kerviel. Leeson. The events that defined operational risk for a generation — none of them have a lifecycle requirement under the current Swiss resilience framework.

3. Your third-party resilience view is fragmented across three regulatory documents

Circular 23/1 (cross-border, §97–100), Circular 23/1 Section V (dependency mapping, §105–109), and Circular 18/3 (outsourcing) together govern third-party operational resilience. With **71% of**

© 2026 Risk Vizon LLC

critical functions depending on third parties, this fragmentation is not an administrative inconvenience. It is a systemic risk.

4. Most institutions have misidentified their critical functions

FINMA Guidance 05/2025 found that approximately **two-thirds of free-text critical function entries were actually processes or resources** — not functions. IT operations, risk management, and back office are enablers of critical functions, not functions themselves. This misreading flows directly from the BCBS/FINMA terminology divergence: BCBS uses 'critical operations' (broad, unified); FINMA uses a three-tier hierarchy of function → process → resource. An institution reading both simultaneously may reasonably conflate them.

5. ICT, Cyber, and Data Risk are siloed where they should be integrated

FINMA created three sub-sections for what BCBS treated as one principle (P7). The interfaces between these domains — where an ICT failure becomes a cyber vulnerability, where a cyber attack compromises critical data — are unaddressed in the circular and, based on SRA forum data, largely unaddressed in industry practice.

6. Governance accountability for resilience is dispersed across three circulars

Circular 17/1 (Corporate Governance), Circular 23/1 (Operational Risks), and Circular 18/3 (Outsourcing) must be read together for a complete picture of board and senior management accountability. FINMA has not produced a consolidated governance map. Boards that rely on a single circular may have significant blind spots.

A Call to Action: For Boards, Executives, and the Regulator

For boards and risk committees

The most important question to ask your CRO right now is not 'are we compliant with FINMA Circular 23/1?' but '**have we approved a board-defined tolerance for disruption for each of our critical functions — and does that tolerance drive our recovery capability design, rather than being derived from it?**'

For executive management

- Build a unified OR framework map that explicitly shows which requirements derive from ORM logic (PSMOR) and which from Resilience logic (d516), and assign clear ownership.
- Integrate your BCM testing and resilience scenario testing into a single programme — not two.
- Extend your incident management framework voluntarily beyond ICT to cover all operational incident types, consistent with BCBS P6.

© 2026 Risk Vizon LLC

For FINMA

- Publish a conceptual clarification note explicitly labelling which requirements in Circular 23/1 derive from ORM logic and which from Resilience logic. Ten pages would resolve confusion that has cost the industry years of misdirected programme work.
- Clarify whether BCM testing (§83–96) and resilience scenario testing (§110–111) can be satisfied by a single integrated programme.
- Consider a unified third-party resilience standard spanning Circular 23/1 and Circular 18/3 — the most operationally consequential structural gap in the Swiss resilience framework.

Closing Reflection: The Distance Between Compliance and Resilience

Operational resilience, properly understood, is not a compliance exercise. It is a strategic capability — the capacity of an institution to continue delivering its most critical functions to its clients and the financial system, through disruptions that stress tests cannot fully anticipate and that regulations can only partially specify.

FINMA Circular 23/1 is a serious, well-intentioned regulatory text. The BCBS framework it transposes is intellectually rigorous and practically necessary. But **compliance with the letter of the circular does not guarantee resilience.** It guarantees that the paperwork is in order when the next disruption arrives.

> **"That is the challenge worth taking to the board."**

I would welcome your perspective — how is your institution navigating the gap between regulatory compliance and genuine operational resilience? Connect on LinkedIn or reach out at anwarul.hasan@riskvizon.com.

Read the complete White Paper:

"Compliant on Paper, Vulnerable in Practice: Why Swiss Financial Institutions Are Failing the Operational Resilience Test"

Available at: **www.riskvizon.com/risk_resources.php**

#OperationalResilience #FINMA #BCBS #SwissBanking #RiskManagement #CyberResilience #BusinessContinuity #RegulatoryCompliance #CRO #BoardGovernance #RiskVizon

ABOUT THE AUTHOR

Anwarul Hasan (MBA, PhD) is the Founder and CEO of Risk Vizon LLC, based in Zurich. With 25+ years of experience in governance and risk management at UBS, KPMG, and Swiss Re, he is the architect of GRIP — the Governance & Risk Intelligence Platform — the most comprehensive, seamlessly integrated and AI-enabled risk management platform, designed to empower boards, regulators and executives to govern, monitor and steer enterprise risks in real time.

anwarul.hasan@riskvizon.com · www.riskvizon.com

© 2026 Risk Vizon LLC