Spotlight 07/24

FINMA WARNS SUPERVISED INSTITUTIONS OF CYBERSECURITY RISKS AND PROVIDES GUIDANCE

The Swiss Financial Market Supervisory Authority ("FINMA") identifies significant gaps in both the awareness of cyber risks and the implementation of corresponding regulatory requirements by financial institutions.

Wenger Vieli Ltd.
Dufourstr. 56
P.O. Box
8034 Zurich
—
Metallstr. 9
P.O. Box
6302 Zug
—
+41 58 958 58 58
spotlight@
wengervieli.ch

In June 2024, FINMA issued two new guidances on operational risks, with a particular focus on cyber risks. This Spotlight provides an overview of the legal obligations of supervised institutions regarding cyber risks, presents FINMA's latest findings and recommendations in this area, and proposes a way forward for financial institutions to effectively manage their evolving cyber risks while ensuring compliance.

FINMA Issues Guidance on Cyber Risks and the Management of Operational Risk Management

In its new guidances, FINMA highlights shortcomings identified in its supervisory activities and outlines its expectations on how supervised institutions should handle cyber risks and establish an appropriate operational risk management framework:

1. FINMA Guidance 03/2024 ("**Cyber Risks**") summarizes FINMA's findings from its supervisory activities on cyber risks. It offers guidance on how to manage cyber risks and clarifies how to report cyber attacks and conduct scenario-based cyber risk exercises. FINMA Guidance 03/2024 is applicable for all institutions supervised by FINMA.
2. FINMA Guidance 04/2024 ("**Management of Operational Risks**") summarizes FINMA's findings from its supervisory activities on operational risks more broadly. It emphasizes the importance of an effective management of operational risks, in particular cyber risks, and clarifies companies' obligations in this area. Although it is limited to fund management companies and managers of collective assets, FINMA Guidance 04/2024 can serve as a guideline for other supervised institutions.

General Requirements for Financial Institutions in Relation to Cyber Risks

The regulatory requirements for financial service providers in relation to cyber risks are based on the following principles:

	Financial Market Law	Data Protection	Information Security
Legal Requirements	Various Financial Market Acts outline the overarching risk management requirements applicable to supervised institutions. Cyber risks are regulated within the operational risk framework mandated for financial institutions.	The Federal Act on Data Protection ("**FADP**"; SR 235.1) regulates the use of personal data, including rules to mitigate and report cyber risks.	The revised Federal Information Security Act ("**ISA**"), expected to come into force on 1 January 2025, requires operators of critical infrastructure to report cyber attacks to the National Cybersecurity Centre ("**NCSC**"). Operators of critical infrastructures include banks, insurance companies and all supervised institutions under the Financial Market Infrastructure Act ("**FinMIA**").
Circular / Ordinance	FINMA Circular on Outsourcing The FINMA Circular 2018/3 "Outsourcing – banks, insurance companies and selected financial institutions under FinIA" sets requirements for financial service providers outsourcing functions, which are essential for compliance with financial market regulation. FINMA Circular Operational Risks The FINMA Circular 2023/1 "Operational risks and resilience – banks" sets guidelines on operational risk and resilience for banks, including cyber risks, critical data protection, and business continuity management.	The Data Protection Ordinance ("**DPO**") provides detailed regulations regarding outsourcing, data security, and the reporting of data security breaches to the Federal Data Protection Commissioner ("**FDPIC**").	
FINMA Guidance	FINMA Guidance on Cyber Attacks The FINMA Guidance 05/2020 on "Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA" outlines the procedures for reporting cyber attacks of substantial importance.		

Findings from FINMA's Supervisory Activities

FINMA found that the scope and frequency of cyber attacks on financial institutions under its supervision have increased significantly in recent years. FINMA identifies serious issues relating to complying with regulatory requirements, which could result in inadequate responses to cyber attacks. The wide-spread outsourcing of IT services further aggravates the situation, with currently more than 50 percent of attacks affecting outsourcing providers.

Some key problems include:

Poor Governance and Management of Cyber Risks

Many financial institutions have not properly integrated cyber risks into their operational risk management framework. There is often a lack of both clear definitions of the specific cyber risks and corresponding risk tolerance as well as a coherent separation between operational management and independent control functions, leading to conflicts of interest.

Inadequate Protective Measures

Unauthorised third parties repeatedly succeeded in obtaining critical data from supervised financial institutions, including access data for key applications. Data loss prevention measures are often limited to customer identification features (e.g. credit card numbers), not covering important information like personal data and business secrets.

Inadequate Detection, Response, and Recovery

FINMA found many institutions lacked adequate response plans for cyber attacks defining clear responsibilities. Business continuity plans, which are intended to safeguard essential functions in the event of an attack, frequently fail to encompass all necessary technical and human resources, complicating the recovery of essential functions during emergencies. Often, regular testing of these plans is not done and many institutions are not aware of their reporting obligations in case of cyber attacks.

Outsourcing to IT service providers

FINMA identified outsourcing as a significant factor to increase vulnerability. Supervised institutions often inadequately select and monitor external services providers, particularly regarding their risk management experience. IT service providers also often address security issues less effectively than the supervised financial institutions. In this context, poor communication between financial institutions and their outsourcing provider may result in security gaps. The inadequate documentation of subcontractor involvement by IT service providers together with insufficient documentation of outsourced services and their criticality by financial institutions in general, leads to significant control gaps within these institutions.

FINMA Recommendations for Minimising Cyber Risks

To address the above shortcomings, FINMA reminds the supervised financial institutions of their obligations to mitigate cyber risks:

Governance and Management of Cyber Risks

Financial institutions must recognize cyber risks as independent risks within their operational risks framework and integrate them into their internal control system ("**ICS**"). The effectiveness of the respective controls must be independently reviewed, evaluated, and documented on a regular basis. Data, particularly customer data, must be identified and protected to ensure availability, confidentiality, and integrity and security measures should be defined according to risk tolerance. Additionally, all responsible functions, the individuals tasked with fulfilling them, and the reporting process must be clearly defined.

Protective Measures

Existing backup and recovery strategies should be regularly reviewed and must include scenarios where protective mechanisms were circumvented by the attackers. In addition, financial institutions should conduct regular training to raise awareness of cyber risks among their workforce.

Detection, Response, and Recovery

Financial institutions must have realistic, regularly updated, and tested response and business continuity plans to maintain essential processes during a crisis. For this purpose, financial institutions need to clearly define tasks, responsibilities, and communication with clients and partners in a cyber incident.

In addition to that, FINMA clarifies its expectations with regards to the reporting of cyber attacks. An initial report must be made within 24 hours of discovering an attack, with an assessment of severity. For attacks deemed "medium," "high," or "severe," a formal report with an investigation must be submitted within 72 hours. For "high" or "severe" attacks, the institutions need to provide an explanation of the attack's success, impact on regulatory requirements and operations, and mitigation measures taken.

Outsourcing

FINMA emphasizes that supervised institutions remain responsible for compliance with regulatory requirements even when outsourcing certain functions. This duty cannot be delegated, requiring careful selection and monitoring of IT service providers. Additionally, the detailed requirements outlined in the FINMA Circular "Outsourcing" must be followed if essential functions are affected.

What to do next?

For several years, cyber risks have been among the main risks identified by FINMA in its yearly Risk Monitor. With respect thereto, FINMA expects supervised institutions to adopt an integrated and systematic approach to addressing cyber risks. This approach must include specific measures for governance, identification, protection, detection, response and recovery of threatened systems and services threatened by cyber risks.

There is no doubt that cyber attacks remain a key challenge for the financial industry in the years to come, and FINMA will closely monitor the efforts of supervised institutions to mitigate these risks.

We recommend all FINMA-supervised institutions to continuously review their cyber defense measures and to explicitly integrate cyber risks into their overall management of operational risks. In addition to financial losses that may occur from cyber attacks, there is also the threat of reputational damage, in particular within the financial services sector.

In this context, the below list of questions may help to identify shortcomings with respect to the institutions' cyber defense and its risk management framework:

- ☐ Have we sufficiently integrated cyber risks into our overall management of operational risk?
- ☐ Have we given cyber risks the necessary priority at management or board level?
- ☐ Have we identified our institution-specific cyber risk threats?
- ☐ Have we defined a process for correctly reporting cyber attacks (e.g. timing, form, addressee)?
- ☐ Do we carry out risk-based and scenario-based cyber exercises (such as annual tabletop exercises, i.e., simulating and playing through a scenario on paper)?
- ☐ Do we maintain an up-to-date inventory of all significant outsourced functions including involved subcontractors (if any)?
- ☐ Do we have up-to-date contracts with our outsourcing providers that address all relevant regulatory requirements?
- ☐ Have we defined a system / process to control our outsourcing partners?
- ☐ Have we defined what constitutes critical data for us?
- ☐ Have we implemented cyber training and awareness programs for employees at all levels of our firm?
- ☐ Is our business continuity management policy still up to date and do the respective processes correspond to the latest threat level?
- ☐ Have we considered whether we fall under the reporting obligations of the ISA as of 1 January 2025 and, if applicable, are we ready to comply with it?

Keyfacts

01 In June 2024, FINMA published two new guidances on operational risks, with a particular focus on cyber risks.

02 FINMA emphasizes the challenges many financial service providers face in establishing adequate governance structures for cyber risks and warns of increased vulnerabilities due to insufficient consideration of security aspects in outsourcing.

Martin Peyer
Partner
m.peyer@wengervieli.ch
+41 58 958 53 53

Claudia Keller
Partner
c.keller@wengervieli.ch
+41 58 958 53 15

Orlando Battaglia
Senior Associate
o.battaglia@wengervieli.ch
+41 58 958 53 69

Matthias Langenegger
Associate
m.langenegger@wengervieli.ch
+41 58 958 53 43

Wenger Vieli is your reliable partner in legal and tax matters. Not only do we pride ourselves on bringing outstanding professional skills, experience, and a sense of responsibility to the table, but we are also highly inquisitive! Where others see obstacles, we see opportunities, find solutions, and open up new horizons. We do this with pleasure. In Switzerland, Europe, and the rest of the world.