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 04/2024

Operational risk management by fund management companies and managers of collective assets

12 June 2024

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

Contents

1 Introduction

To protect investors effectively, fund management companies and managers of collective assets (hereafter institutions) must have a properly functioning risk management system.

Risk management encompasses all material risks the institution, and the collective investments and other assets managed by it, are or could be exposed to in the course of its business activities (cf. Arts. 9 and 26 Financial Institutions Act [FinIA; SR *954.1*], Art. 12 para. 4, Arts. 41 and 57 Financial Institutions Ordinance [FinIO; SR *954.11*] and Arts. 8 ff. and 18 FINMA Financial Institutions Ordinance [FinIO-FINMA; SR *954.111*]).

Operational risks form part of these material risks. As for other institutions supervised by FINMA, the operational risks of fund management companies and managers of collective assets are increasing, as for example reports of cyber attacks demonstrate. At the same time, in licensing procedures and its ongoing supervision FINMA is increasingly noticing weaknesses and deficiencies in operational risk management by fund management companies and managers of collective assets.

This guidance is therefore addressed to these institutions to remind them of the importance of managing operational risks appropriately and highlighting possible action to take.

In accordance with FINMA Circular 2023/1 “Operational risks and resilience – banks”[1], operational risk is defined as the risk of financial loss resulting from inadequate or failed internal processes or systems, inappropriate actions or mistakes by people, or external events. This includes financial losses that can result from legal or compliance risks. Operational risk management must also take account of other types of harm[2] if these could also result in financial loss. However, it does not include strategic risk.

2 Examples of weaknesses and deficiencies identified by FINMA

In this section we list some examples of recently identified weaknesses and deficiencies in operational risk management.

[1] www.finma.ch > Documentation > Circulars.

[2] For example adverse reputational effects, possible loss of confidence and loss of clients, adverse impact on the market, adverse regulatory impact (e.g. possible loss of licence).

2.1 In the area of processes and systems in general

Due to the absence of controls, or controls not being carried out on time, mistakes in entering transactions or in transaction statements were only discovered after a loss had occurred.

2.2 In the area of information and communications technology (ICT) and data security

When launching cloud solutions to store client and corporate data, the issues of selection and in particular monitoring of providers of cloud services, access rights, data security and inclusion in business continuity management and business continuity plans were not considered or given insufficient consideration.

There was inadequate identification, or none at all, of the main infrastructure, particularly for ICT, to perform the institution's significant activities and therefore this infrastructure was insufficiently protected and was not given appropriate consideration in the business continuity plans.

2.3 In the area of cyber risks

Unauthorised third parties gained access to institutions' critical data through successful phishing attacks, including access data for significant applications. Attempts were made to carry out unauthorised transactions with this stolen data.

Institutions who had outsourced their accounting to an external service provider temporarily lost oversight and control over their financial situation after successful cyber attacks on the provider and were thus unable to monitor their capital position, for example.

Although institutions were able to identify cyber attacks quickly, they did not have plans for how to respond to these attacks and what the responsibilities and reporting lines were within the organisation in these cases.

Finally, institutions were unaware that, as set out in FINMA Guidance 05/2020 "Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA"[3], they are required to report cyber attacks to FINMA. In addition, they were also not aware that they have a duty to report breaches of data security to the Federal Data Protection and Information Commissioner.[4]

[3] www.finma.ch > Documentation > FINMA Guidance.

[4] cf. the duty to report data security breaches to the Federal Data Protection and Information Commissioner in accordance with Art. 24 of the Federal Act on Data Protection (FADP; SR **235.1**), see Online service for data breach reporting (Art. 24 FADP).

2.4 In the area of business continuity management

The business continuity plans did not capture all of the material resources required to perform the current significant activities, particularly in respect of human and technical resources. Thus institutions were unable to ensure they could maintain or rapidly resume their main activities in the event of a crisis.

Business continuity plans were not tested or not tested regularly, which led or could lead to considerable delays in remediating losses if they occurred.

2.5 In the area of legal and compliance risks

Institutions used financial instruments or investment techniques in individual wealth management that were unsuitable for the clients involved or did not comply with the contractual agreements.

Institutions that provide wealth management services to individual clients did not pay sufficient regard to the client's place of residence in the risk analysis required under anti-money laundering legislation.

This was in spite of the fact that institutions had both internal guidelines for cross-border activities and country handbooks. However, the controls and lines of responsibility contained in these documents were not carried out and adhered to, or only inadequately.

2.6 In the area of significant outsourced activities

When selecting service providers to which operational risk management was to be outsourced, too little weight was put on the knowledge and experience of these service providers in managing operational risks (cf. margin nos. 16-21 FINMA Circular 2018/3 "Outsourcing"[5] on the requirements for selecting, instructing and monitoring service providers).

Outsourced activities were not recorded, or incorrectly recorded (cf. margin nos. 14-15.1 FINMA Circular 2018/3 "Outsourcing" on drawing up inventories of outsourced functions). This created gaps in monitoring, or these outsourced activities were not incorporated sufficiently into operational risk management.

[5] www.finma.ch > Documentation > Circulars.

3 General requirements for risk management

3.1 Risk management in general

To avoid the abovementioned and other similar weaknesses and deficiencies, FINMA is therefore reminding fund management companies and managers of collective investments of the general requirements for appropriate risk management.

The governing body for guidance, supervision and control, usually the board of directors, is responsible for laying down the policies for managing all material risks the institution is exposed to through its business activities and the assets managed by it in internal guidelines. It also has to determine the institution's risk tolerance.

Based on the policies laid down by the board of directors, executive management is required to develop suitable guidelines, procedures and processes for identifying, managing and monitoring risks. It must also define the functions or persons responsible and ensure there is appropriate regular reporting to the board of directors.

The board of directors and the executive management are required to review the effectiveness and suitability of its risk management principles, risk tolerance, guidelines, procedures and processes regularly, particularly when there are changes in business activities or the organisational structure.

3.2 Operational risk management as a component of risk management

Operational risks are among the main risks for fund management companies and managers of collective assets and the assets they manage. Hence the requirements set out in this section apply equally to operational risk management. Particularly from a human resources perspective, this means that the persons responsible for managing operational risks must have the required knowledge and experience.

4 Operational risk management

4.1 General principles for operational risk management and organisation

Taking account of an institution's actual business activities and organisation is an essential prerequisite for managing operational risk effectively on an institution-wide basis. There needs to be a particular focus on the processes

and procedures used to perform these activities, the human and technical resources deployed and the data required.

When designing operating processes and procedures, the institution must build in appropriate safeguards and controls (e.g. the dual signatory principle) to ensure the processes and procedures are effective and reliable.

4.2 Specific elements of operational risk management

4.2.1 ICT risks

The basis for effective management of ICT risks is an inventory of the main hardware and software components used by the institution in the processes and procedures for performing its main activities.

The institution lays down the risk tolerance for these key hardware and software components and takes the measures required to ensure the defined availability, confidentiality and integrity.

4.2.2 Critical data risks

Data requiring special protection (e.g. client data), or which is critical for the institution's activities, must be identified and appropriate measures need to be in place to protect its availability, integrity and confidentiality.

This includes clearly setting out the tasks, responsibilities, reporting lines and controls relating to how the critical data is managed.

4.2.3 Cyber risks

Based on its business activities and organisation, an institution must analyse and identify the potential threats from cyber attacks. It must then take appropriate protective measures and ensure its ICT infrastructure is monitored appropriately.

The institution is expected to regularly train and raise awareness among staff about how to deal with cyber risks.

The institution must have a plan of action for how it would resume regular business operations quickly in the event of a successful or at least partly successful cyber attack. It must also ensure that it meets its obligations to report cyber attacks.[6]

[6] Cf. obligation to report cyber attacks in accordance with Art. 29 para. 2 FINMASA and FINMA Guidance 05/2020 (see footnote 3) and obligation to report breaches of data security to the Federal

Particularly when dealing with cyber risks, it is important that the institution has clearly defined the tasks, responsibilities and reporting lines and in doing so also takes account of its duty to communicate, particularly with affected clients, business partners and other persons as appropriate.

4.2.4 Business continuity management

An institution must produce a business continuity plan commensurate with its business activities and organisation to maintain and restore the significant processes and procedures for its business operations in the event of a crisis.

It is important that the business continuity plan is reviewed periodically and updated as appropriate. Furthermore, a review and potential update of the business continuity plan is likely to be necessary if changes are made to the institution's business activities and organisation.

Business continuity plans should be tested periodically, particularly by institutions with large or complex business activities.

Finally, it is important that an institution has a clear communications strategy for emergencies and has determined clear responsibilities and reporting lines.

4.2.5 Management of legal and compliance risks, particularly in cross-border business

If an institution provides cross-border services or distributes financial instruments across borders, it must ensure that its appropriately identifies, limits and monitors the resultant risks.

The institution must analyse the legal framework for its cross-border services and the cross-border distribution of financial instruments, identify the resultant risks and take the required risk mitigation measures.

The relevant legal position in the countries concerned must be monitored continuously and the risk mitigation measures updated if required.

4.2.6 Operational risk management for outsourcing

4.2.6.1 Outsourcing of risk management and compliance

The institution must ensure that appropriate measures to manage operational risks are in place in the event that risk management and compliance is outsourced to third parties. When selecting third parties to

Data Protection and Information Commissioner in accordance with Art. 24 of the Federal Act on Data Protection (see footnote 4).

provide risk management, the institution must also have regard to their knowledge and experience of operational risk management.

4.2.6.2 Outsourcing of significant activities

If the institution outsources other significant activities for its business to third parties or obtains resources from third parties for material processes and systems, it must ensure the requirements in accordance with FINMA Circular 2018/3 “Outsourcing”[7] are met (particularly as regards keeping an inventory of outsourced functions and selecting, instructing and monitoring the service provider). The institution must also ensure that outsourced functions are included in operational risk management.

[7] See footnote 5.