SFAMA Swiss Funds & Asset Management Association

Specialist Recommendation

Specialist Recommendation on Risk Management

7 September 2018

I Basic principles, objectives, and binding force

This Specialist Recommendation forms part of the Swiss fund industry's self-regulation regime. It is based on the Code of Conduct of the Swiss Funds & Asset Management Association SFAMA (SFAMA Code of Conduct). **1**

This Specialist Recommendation is intended to clarify the regulatory requirements within the scope of the Collective Investment Schemes Act (CISA) with regard to risk management (Art. 12a Collective Investment Schemes Ordinance (CISO)). The focus is on the risk management function, which is separate from the operating units (second line of defense), as defined in margin no. 14 below. **2**

No standard has yet been established in the Swiss fund and asset management industry for implementing the requirements pertaining to risk management. The purpose of this document is to define such industry standards, taking due account of each company's size and complexity as well as its specific areas of activity. **3**

This Specialist Recommendation applies to all asset managers of collective investment schemes under Art. 18 et seqq. CISA, fund management companies under Art. 28 et seqq. CISA, investment companies with variable capital (SICAVs) under Art. 36 et seqq. CISA, investment companies with fixed capital (SICAFs) under Art. 110 et seqq. CISA, limited partnerships for collective investment under Art. 98 et seqq. CISA, and all institutions exempted from the duty to obtain authorization under Art. 8 para. 1 CISO. The above are referred to collectively as "*CISA Institutions*". **4**

Additional Swiss or foreign regulations and contractual terms may apply to individual CISA Institutions. A financial service provider's adherence to the rules set out in this Specialist Recommendation does not release it from the obligation to comply with such regulations or contractual terms. The purpose of this document is to establish standards that are compatible with other Swiss and foreign rules. **5**

CISA Institutions that delegate or subdelegate investment decisions and/or other specific tasks must still ensure compliance with the provisions of this Specialist Recommendation as set out below. **6**

This Specialist Recommendation does not restrict the Swiss Financial Market Supervisory Authority FINMA's scope to grant derogations from the legal requirements in justified instances (Art. 12a para. 4 CISO). **7**

II Specialist Recommendation

A General provisions

1. Basic principles

CISA Institutions must ensure that they have proper and appropriate risk management, an internal control system (ICS), and compliance covering their entire business activities (Art. 12a para. 1 CISO). This includes risks relating to the institution itself as well as those relating to the collective investment schemes it manages and other assets managed on a mandate basis (Art. 68 para. 2 CISO-FINMA). **8**

This Specialist Recommendation follows a holistic approach whereby both investment risks and enterprise risks must be taken into account. **9**

Risk management must be organized so that all material risks can be adequately identified, assessed, controlled, and monitored (Art. 12a para. 2 CISO). Material risks are all risks with the potential to have a significant impact on the CISA Institution, its business activities, and/or the assets it manages. The basis for materiality must be appropriately documented and, where possible and expedient, quantified. **10**

Appropriate risk management and risk control principles as well as the organization of risk management and risk control must be set down in internal guidelines (Art. 68 para. 1 CISO-FINMA). These must take account of the nature, scope, and complexity of the transactions carried out, the collective investment schemes managed, and the assets managed under the terms of mandates (Art. 68 para. 4 CISO-FINMA). **11**

The appropriateness and effectiveness of the risk management principles and the procedures and methods defined must be reviewed and refined on a regular basis. **12**

2. Definitions

For the purposes of this document, “risk management” refers to the process (identifying, assessing, controlling, and monitoring) and to governance. **13**

For the purposes of this document, “risk management function” refers to the organizational unit responsible for risk management. The risk management function identifies, assesses, controls, and monitors material risks. **14**

“Enterprise risks” are all company-wide risks relating to a CISA Institution. They may, for example, be detrimental to the following: **15**

- strategic and operating targets, i.e. the effective and economical use of resources
- reporting, in particular its reliability
- compliance, specifically with the applicable laws and other provisions

For the purposes of this document, “risk tolerance” in the context of enterprise risk management refers to the entire aggregated risk a company is willing to bear. Risk tolerance is limited by the company’s ability to bear risk, which is measured in terms of its available capital. **16**

“Investment risks” are those that may arise in connection with investments made either by the collective investment schemes a company manages or under mandates, including in particular market, liquidity, and counterparty risks. **17**

"Market risks" are material risks arising from an investment policy as well as those that are not directly expected in connection with that policy. **18**

Market risks that are not directly expected in connection with an investment policy are exposures that can lead to disproportionately high, unintentional or even insufficient fluctuations in value in relation to the policy. **19**

"Liquidity risk" refers to the risk that it may not be possible to fulfill redemptions by a collective investment scheme's investors within the prescribed deadline or without creating a disadvantage for the remaining investors. **20**

"Counterparty risks" are those that may arise due to counterparties defaulting in connection with spot and over-the-counter derivatives transactions or other investment techniques such as securities lending. **21**

"Risk dialog" refers to the discussion of risks between the risk management function, the operating units, and the governing bodies. This may result in a risk being accepted, measures to reduce the risk being agreed or a decision to escalate the risk. **22**

B Governance and organization of risk management

1. Governance

The CISA Institution must ensure an appropriate and clearly documented separation of duties between the board of directors, the executive board, the operating units, and the risk management function. **23**

The board of directors must put in place an internal control system based on systematic risk analysis and monitor it in such a way as to ensure that all of the CISA Institution's material risks are appropriately identified, assessed, controlled, and monitored (Art. 67 para. 1 CISO-FINMA). **24**

The CISA Institution's board of directors defines the company's risk tolerance and risk policy. It discusses the key issues concerning risks, makes fundamental decisions on risks, and ultimately oversees the implementation of such decisions. It ensures compliance with the risk management principles and assesses the appropriateness and effectiveness of measures to remedy any shortcomings in the risk management process. **25**

The executive board implements the decisions made by the board of directors concerning the setting up, maintenance, and regular review of the ICS. It develops suitable processes to implement the control activities that are to be integrated into working processes and to control risks (Art. 67 para 2 CISO-FINMA). **26**

The executive board implements the risk policy defined by the board of directors and issues directives and guidelines for this purpose. It is responsible for risk control and oversees the work of the risk management function. The executive board or any risk committee it forms serves as the next escalation level for the risk management function. The risk management function regularly informs the executive board and the board of directors or any risk committees about risks. **27**

Compliance with the defined risk management principles and processes as well as the appropriateness and effectiveness of the measures to remedy any shortcomings in the risk management process are part of the reporting to the board of directors and executive board **28**

or any risk committees.

The risk management function (second line of defense) identifies, assesses, controls, and monitors the risks of the operating units. It ensures adequate reporting and escalates risks as required (see margin no. 33). **29**

The operating units (first line of defense) identify, assess, control, and monitor the risks arising in connection with their activities and the applicable requirements and are responsible for these. **30**

2. Organization and positioning of the risk management function

The risk management function must be functionally and hierarchically separated from the operating units, in particular the investment decisions function (portfolio management) (Art. 12a para. 3 CISO and Art. 70 para. 3 CISO-FINMA). The risk management function may employ the data and systems of the operating units, provided the integrity of the data and calculation models used is assured. **31**

It must be organized so as to ensure effective risk management in practice. It may be deemed to be adequately organized if it has appropriate resources, expertise, information, and systems at its disposal in relation to the actual business activities. The risk management function's expertise must be equivalent to that of the operating units in terms of breadth (i.e. topics covered), but not in terms of depth (i.e. degree of specialization). However, the risk management function must be in a position to identify and assess risks. **32**

Adequate escalation processes and decision-making authorities must be defined. **33**

3. Delegation of risk management

Where risk management is delegated to a third party, the delegating CISA Institution must have the necessary personnel and expertise to select, instruct, and monitor the third party and to manage the risks associated with it (Art. 66 para. 3 let. b CISO-FINMA). However, this does not mean that the delegating CISA Institution must duplicate the delegated activity. **34**

The delegated tasks must be set out in a written agreement including a precise description of the delegated tasks as well as the powers and responsibilities, any authorities in respect of further delegation, the agent's duty to give an account of its activities, and the control rights of the delegating CISA Institution (Art. 66 para. 2 CISO-FINMA). **35**

4. Delegation of asset management

Where a CISA Institution delegates asset management to a third party, the measures qualifying as appropriate in connection with the organization of risk management in its specific case are determined not only by the delegated activity (asset management) and the corresponding tasks, but also by the structure and capabilities of the third party. A risk-based approach must be followed whereby the monitoring concept is determined based on the organization of the third party's risk management function, subjected to a regular risk assessment (as a rule once a year), and adjusted if necessary. In such cases, it is not necessary for both the delegating CISA Institution and the third party to ensure cumulatively that all measures are in place for appropriate risk management in relation to investment risks (Art. 68 para. 2 let. b, Art. 68 para. 3 let. c, and Art. 70 para. 2 let. b CISO-FINMA). **36**

C Identifying, assessing, controlling, and monitoring risks

1. General provisions

Material enterprise and investment risks must be identified, assessed, controlled, monitored, and documented. Materiality is determined on the basis of potential losses, plausibility, and probability. **37**

The methods used to identify and assess risks must be constantly refined. **38**

The risk management process must be documented, and a risk dialog must take place. All decisions must be set out in writing. **39**

2. Enterprise risks

A risk catalog must be drawn up as a basis for systematically identifying, assessing, and controlling risks. **40**

The risks identified must be appropriately assessed. Both the extent (potential losses) and the probability of each risk must be taken into account. **41**

The CISA Institution must take suitable measures to control risks such that they do not exceed its risk tolerance. **42**

The risk management function must be consulted whenever changes are made to the CISA Institution's business activities or organization. **43**

The CISA Institution must define its risk tolerance in order to assess the effectiveness of risk control. The risk tolerance must be controlled and monitored using quantitative or qualitative restrictions (limits, metrics or key performance indicators). **44**

With regard to monitoring, a risk report must be produced periodically (at least once a year) and signed off by the board of directors. The report must at least cover the following topics: **45**

- identifying and assessing material risks
- a statement on the effectiveness and completeness of measures to control risk
- an explanation of residual risk (in quantitative and/or qualitative terms), together with a comparison against the risk tolerance
- a statement on the future development of the risk situation
- the implementation status of the defined measures

The implementation of the measures defined to control risks must be monitored. **46**

3. Investment risks

The CISA Institution must produce a risk profile for each collective investment scheme or asset management mandate. This is derived from the investment objectives and the investments, investment techniques and instruments, investment limits, and risk budget defined in the investment policy. The risk measurement process must be aligned with the investment objective, investment policy, and risk profile. **47**

Quantitative limits must be used to assess and control market risks arising from the investment policy (margin no. 18). **48**

Market risks that are not directly expected in connection with the investment policy must be identified and assessed using suitable metrics in the context of overall risk, overall exposure, assets under management or expected performance/outperformance. Stress scenarios must be taken into account when assessing these risks, which may be controlled using limits or through a risk dialog. **49**

The liquidity risk for each collective investment scheme must be calculated using suitable criteria that provide meaningful quantitative information. A key criterion in this respect is the liquidity gap that results from comparing the time it would take to sell individual positions held by the collective investment scheme against the redemption period communicated to investors or expected redemption behavior for the purpose of liquidity planning. The materiality of the liquidity risk and the liquidity gap must be assessed. **50**

Depending on the materiality, preventive, risk-reducing measures must be taken and documented. The redemption policy and related measures (e.g. gating) for each collective investment scheme must also be determined and documented for investors. **51**

Counterparty risk is the risk of a collective investment scheme or asset management mandate incurring losses due to a business partner (counterparty) defaulting. In addition to concentration limits for each collective investment scheme, counterparty risks must be controlled and monitored with the aid of limits for each counterparty in relation to the entire assets managed on a fiduciary basis by the CISA Institution. **52**

An appropriate risk dialog must be conducted between the risk management and portfolio management functions. This dialog must address the issues of excessive, unknowing, and insufficient risk-taking and serve to decide whether specific risks are accepted or whether measures are to be taken to mitigate them. Decisions must be documented, and the outcomes of the risk dialog must be communicated to a superior body (e.g. risk committee or executive board) in a suitable form. Any disagreements must be handled via the defined escalation and decision-making process (margin no. 33). **53**

The defined limits used to monitor investment risks must be reviewed on a regular basis. **54**

D Legal nature

This Specialist Recommendation is a recommendation from SFAMA for the Swiss funds and asset management industry. The Swiss Financial Market Supervisory Authority FINMA has not formally acknowledged it or recognized it as a minimum standard in accordance with FINMA Circular 2008/10 “Self-regulation as a minimum standard”. Within the scope of its powers under supervisory law, FINMA may impose additional or different requirements on institutions it supervises. **55**

E Further developments

SFAMA follows national and international regulatory developments in the area of risk management closely and will update this Specialist Recommendation as necessary. Any amendments will be announced via the usual SFAMA communication channels. **56**

This Specialist Recommendation will also be reviewed with regard to the need for adjustment in connection with the entry into force of the Financial Services Act (FinSA), the Financial Institutions Act (FinIA), and the related changes to the legislation on collective investment schemes. **57**

F Entry into force

This Specialist Recommendation was adopted by the SFAMA Board of Directors on 7 September 2018. It enters into force with immediate effect. **58**

CONTENTS