

Leaflet minimum content of risk management/ICS for financial institutions according to Art. 17 FinIA

1. General remarks

All financial institutions shall be appropriately organized in accordance with the Federal Act on Financial Institutions (FinIA). In this regard, the supervisory organizations and the Swiss Financial Market Supervisory Authority FINMA particularly check that the financial institutions have set up comprehensive and appropriate directives concerning its planned and performed activities and particularly defined basic principles concerning risk management and controlling.

As part of the risk management and controlling, the latter separately presented in an internal risk control, it shall be outlined that the institution is familiar with the activities, existing clients, financial instruments and strategies used as well as the operational organization and corresponding risks for its personnel, all of which shall be identified, classified and categorized.

This leaflet is not exhaustive but lists all aspects which usually need to be laid down and reflect the minimum content from OSFINcontrol Ltd's perspective. The way in which risk management, incl. ICS, is regulated, may vary. OSFINcontrol Ltd reviews compliance with above-mentioned aspects on the occasion of the (preliminary) affiliation as well as in the context of the ongoing supervision. Risk management and ICS also form mandatory documents for approval by the Swiss Financial Market Authority FINMA.

2. Content of directives

	Subjects to be addressed	Remarks
1.	Objective / basics / target	The directives shall initially describe the subject area. The objective shall describe what is regulated by the directives. Furthermore, the directives shall reference the relevant underlying principles. Finally, the directives shall clarify to whom they do apply (usually to all employees of the financial institution, including its highest governing body). <i>Note: the risk management directives do not necessarily list all risks relevant to the institution. Yet, it forms the basis and describes the principles according to which all risks are to be addressed. Further rules on how to deal with specific risks are then derived from other directives dealing with specific topics (e.g. organizational regulations, directives concerning conflicts of interest, directives concerning portfolio management, AMLA directives, etc.)</i>
2.	Definition of responsibilities	The directives shall specify under which body's responsibility within the financial institution the different aspects of risk management do fall.

		The highest governing body is generally responsible for the identification, categorization and classification of the financial institution's risks (according to occurrence probability and severity). Based on such classification, top risks shall be defined. Appropriate control and monitoring measures must then be defined for all risks. Finally, the entire risk situation of the institution should be reassessed at least once a year. At this point in time, it should be checked additionally that the defined risk management is still up-to-date and effective. The management is responsible for the implementation of the defined risk control. It is its responsibility to monitor the risk landscape identified by the highest governing body in the operative business and to create appropriate, regular reports about such monitoring. Depending on the organizational structure, a separate (independent) risk management shall be created within the business for these tasks – or the activity outsourced to external third parties. Even in the latter case, the implementation shall be monitored and approved by the highest governing body.
3.	Definition and principles of risk management	The principles of risk management shall be outlined. These should include definition of certain terms and activities implementation of which is of fundamental importance for the risk management of the financial institution: - How is it defined and what is a risk - Which functions do fall under the area of risk management and risk controlling - Implementation of internal control system ICS Risk assessment determines on how to address and monitor possible risks by the financial institution. Implementation of monitoring is set forth in further directives which deal with the respective topics and clarify with which (internal) processes the relevant risks are avoided, monitored and controlled. The institution should also determine the principles according to which certain risks are to be monitored (principle of risk-based approach vs. control of each individual transaction). The principles chosen must be in line with the business strategy, size of the organization, client base and personnel.
4.	List and description of the risks identified in each case	All possible risks identified for the specific business and financial institution shall be described. Roughly, distinction can be made as follows: - risks arising from business activity (on the one hand with regard to the chosen business strategy, i.e. specifically with regard to market risks, risks associated with the financial instruments and investment strategies used, credit risks, risks associated with investment products such as collective investment schemes, etc.) - risks arising from business organization (operational risks: personnel, finances, reputation, legal risks, incorrect execution of orders, etc.)

		- risks arising from specific client mandate (different duties apply to asset management activities compared to pure advisory activities). - risks arising from international context of the relationship supported. - risks arising from international elements concerning custodian banks.
5.	Internal control system ICS	<i>Separate document</i> Description on how to avoid, monitor, control or reduce risks. The ICS shall encompass all identified risks. It represents an overview and summary of all risks relevant to the institution which are to be monitored continuously. Consequently, we recommend to do an inventory and description of internal processes in order to derive the resulting (control) obligations. For any risk schedule, we recommend to divide the overview into the following columns (minimum content): - risk: name and description - reference to the underlying directives (basis) - identification of business unit from which the respective risk may arise - responsibility for risk monitoring - if needed, description of at least required control steps - interval of control – how regularly is the risk to be checked / monitored - reporting-lines: to whom and in which format reporting shall be done - deadline for next inspection (to be updated regularly)