

Subject: **Risk Management Guideline**

Number: **3/2020**

Date: **November 2020**

Scope: **All Non-Bank Financial Services Providers**

Table of Contents

1. Introduction 2
   Definitions 2
2. Objectives 2
3. Enterprise Risk Management Framework 3
4. Role of Board and Senior Management 3
   4.1 Board 3
   4.2 Senior Management 4
5. Risk Assessment 5
   5.1 Types of Risks 5
   5.2 Risk Measurement 6
   5.3 Own Risk and Solvency Assessment 6
6. Risk Appetite and Limits 7
   6.1 Risk Appetite Framework 7
   6.2 Risk Appetite Statement 8
   6.3 Risk Limits 9
   6.4 Relationship to Other Risk Management Strategies and Policies 9
7. Risk Management Systems and Procedures 9
   7.1 Organisation 10
   7.2 Resources 10
   7.3 Operational Policies, Procedures and Practices 10
8. Monitoring and Reporting 11
   8.1 Management Information Systems 11
   8.2 Operational Reports 11
   8.3 Reporting to the Board and Senior Management 12
9. Controls 12
   9.1 Internal Controls System 12
   9.2 Risk Management Function 13
   9.3 Internal Audit Function 14
   9.4 Periodic Review of the Effectiveness of Internal Controls 15

1. Introduction

Risk management by a financial services provider (an FSP) is the process of identifying, monitoring, assessing, and controlling inherent risk in the conduct of its business. While risk-taking is an inherent element of business, and indeed profits are in part the reward for successful risk taking, excessive and poorly managed risk can lead to losses and thus impair the financial soundness of an FSP. It can result in direct loss of earnings and erosion of capital or may result in imposition of constraints on an FSP's ability to meet its business objectives. These constraints could hinder an FSP's capability to conduct its business or to take advantage of opportunities that would enhance its business. As such, managers of FSPs are expected to ensure that the risks an FSP is taking are warranted.

Risks are considered warranted when they are understandable, measurable, controllable and within an FSP's capacity to readily withstand adverse results. Sound risk management systems enable managers of FSPs to take risks knowingly, reduce risks where appropriate and strive to prepare for a future, which by its nature cannot be predicted with absolute certainty. Risk management is a discipline at the core of every FSP and encompasses all activities that affect its risk profile. Managers of FSPs should attach considerable importance to improve the ability to identify, monitor, measure, and control the overall risks assumed.

Definitions

Stakeholder means, in relation to an FSP, a client, customer or prospective client or customer of the FSP.

2. Objectives

The Financial Services Regulatory Authority (the FSRA) places significant emphasis on the adequacy of an FSP's risk management capacity. The FSRA therefore puts forward this document for the purpose of providing guidelines to all FSPs on risk management systems that are expected to be in place.

This document sets out the FSRA's expectations regarding the risk management framework of an FSP. For the purpose of these guidelines, risk in an FSP refers to the possibility that the outcome of an action or event could bring adverse impacts on the FSP's capital, earnings or its viability. This is in line with the provisions of Section 6(1)(b) and Section 30(1)(e) of the Financial Services regulatory Authority Act, 2010.

The guidelines are in line with internationally accepted risk management principles and best practices, for example:

- Insurance Core Principles ICP 8: Risk Management & Internal Controls and ICP 16: Enterprise Risk Management; and
- Basel Core Principle for Effective Banking Supervision BCP 15: Risk Management Process.

These guidelines should be read jointly with the guidelines on the management of specific types of risks, including any industry-specific guidelines[1]. The overarching principles provided under these guidelines are applicable to all FSPs. FSPs are expected to apply these principles taking into account the size, complexity, risk profile and nature of their activities.

3. Enterprise Risk Management Framework

An FSP should establish, implement, and maintain a documented enterprise risk management framework that is capable of promptly identifying, measuring, assessing, reporting, monitoring and controlling all sources of risks that could have a material impact on its operations in a timely manner. The enterprise risk management framework should document the probability, potential impact and duration of each risk. It should be appropriate taking into account the size, complexity, risk profile and nature of the FSP's activities.

It is good practice for an FSP to describe the key elements of its risk management framework in a risk management strategy (RMS), which should be approved by the Board.

4. Role of Board and Senior Management

4.1 Board

The board of an FSP is ultimately responsible for the prudent management of risks of the FSP and the risk management framework. Accordingly, it should approve the overall business strategies and significant policies of the FSP, including those related to managing and taking risks, and should also ensure that senior management is fully capable of managing the activities that the FSP undertakes. While all boards are responsible for understanding the nature of the risks significant to their FSPs and for ensuring that management is taking the steps necessary to

[1] For example, the Guidelines for Savings and Credit Cooperative Societies (November 2019) touch on risk management topics as well as the Reinsurance and Investment Guidelines, which also deal with issues of risk management.

identify, measure, monitor, and control these risks, the level of technical knowledge required of directors may vary depending on the particular circumstances at the FSP.

The board should receive reports that identify the size and significance of the risks in terms that are meaningful to them. The board should take further steps to develop an appropriate understanding of the risks, possibly through briefings from auditors and external experts. Using this knowledge and information, the board should provide clear guidance regarding the acceptable level of exposures and ensure that senior management implements the procedures and controls necessary to comply with adopted policies. The board should ensure that the FSP complies with the requirements of legislation related to risk management and acts in a manner consistent with this guideline.

The board should ensure that adequate resources, expertise and support are provided for the effective implementation of the FSP's risk management strategy, policies and procedures. The board should also approve changes and exceptions to such policies. The board should ensure that the risk management framework is reviewed regularly and updated to maintain its effectiveness.

4.2 Senior Management

Senior management should develop, document, and seek board approval for the risk management framework, strategy, and policies. Senior management is responsible for developing operational procedures and implementing strategies in a manner that limits risks associated with each strategy and that ensures compliance with laws and regulations on both a long-term and day-to-day basis. Accordingly, senior management should possess sufficient knowledge of all major business activities of the FSP, to ensure that appropriate policies, controls, and risk monitoring systems are in place and that accountability and lines of authority are clearly delineated.

Senior management is also responsible for establishing and communicating a strong awareness of the policies and procedures, and the need for effective internal controls and high ethical standards. Senior management should establish and implement remuneration policies that avoid potential incentives for unauthorised risk taking.

Senior management should monitor and assess the management of the FSP's risks and report to the board, both regularly and in response to changes in the risks of FSPs.

5. Risk Assessment

5.1 Types of Risks

An FSP should identify, define and assess the materiality of all known, reasonably foreseeable, emerging and other relevant risks that may have an impact on its ability to continue operations, in both normal and stressed situations. An FSP's identified risks are expected to evolve as its business activities and environment evolve. The assessment should include all material risks, including risks that are not easily quantifiable. Some risks can be broken down into other more discrete risks and may take different forms depending on the nature of the business and activities of an FSP.

Categories in which types of risk are classified can vary from one FSP to another. Examples of some commonly used categories include credit risk, market risk, liquidity, insurance risk, operational risk, regulatory compliance risk, and strategic risk.

Credit Risk: Credit risk arises from a counterparty's potential inability or unwillingness to fully meet its on and/or off-balance sheet contractual obligations. Exposure to this risk occurs any time funds are extended, committed, or invested through actual or implied contractual agreements.

Market Risk: Market risk arises from potential changes in market rates, prices or liquidity in various markets such as for interest rates, credit, foreign exchange, equities, and commodities. Exposure to this risk results from trading, investment, and other business activities which create on- and off-balance sheet positions.

Liquidity Risk: Liquidity risk is the exposure to loss in the event that sufficient liquid assets will be unavailable, or will be available only at excessive cost, to meet the cash flow requirements of obligations when they are due.

Insurance Risk: Insurance risk arises from the potential for claims or pay-outs to be made to policyholders or beneficiaries. Exposure to this risk results from adverse events occurring under specified perils and conditions covered by the terms of an insurance policy or the rules of a retirement fund.

Operational Risk: Operational risk arises from potential problems due to inadequate or failed internal processes, people and systems, or from external events. Operational risk includes legal risk, i.e., potential unfavourable legal proceedings.

Regulatory Compliance Risk: Regulatory compliance risk arises from an FSP's potential non-conformance with laws, rules, regulations, prescribed practices, or ethical standards in any jurisdiction in which it operates.

Strategic Risk: Strategic risk arises from an FSP's potential inability to implement appropriate business plans and strategies, make decisions, allocate resources, or adapt to changes in its business environment, such as competition and economic conditions.

Reputational Risk: This is the chance of losses due to a declining reputation as a result of practices or incidents that are perceived as dishonest or disrespectful or incompetent.

5.2 Risk Measurement

Once risks have been identified, they should be measured in order to determine their potential impact on the FSP's earnings, capital and solvency. This can be done using various tools and techniques, ranging from simple to sophisticated models, and including stress testing. Where a risk is not readily quantifiable, an FSP should undertake a qualitative assessment that is appropriate to the risk and sufficiently detailed so that it can be useful for risk management.

Accurate and timely measurement of risks is essential to effective risk management systems. An FSP that does not have a risk measurement system has limited ability to control or monitor risk levels. An FSP should periodically test its risk measurement tools to make sure they are adequate and reliable. Good risk measurement systems assess the risks of both individual transactions and portfolios.

FSPs should document underlying assumptions, processes and key considerations with regard to the drivers, the assessment, measurement and mitigants in place for each risk.

5.3 Own Risk and Solvency Assessment

It is good practice for an FSP, as part of its risk management process, to perform own risk and solvency assessments (ORSAs). The ORSA should serve as a tool to enhance an FSP's understanding of the interrelationships between its risk profile and capital needs. The ORSA should consider all reasonably foreseeable and relevant material risks, be forward-looking and be congruent with an FSP's business and strategic planning. As the ORSA is a dynamic forward-looking process, stress and scenario testing should be an important component used in an FSP's determination of its own capital needs and as it sets and evaluates the adequacy of its internal targets and operating capital level throughout the business cycle.

The ORSA can be prepared either on an individual FSP basis or on a group basis. When an FSP's business and risk profiles or circumstances are not adequately reflected in a group ORSA, it should have a separate ORSA.

An ORSA would typically contain, at a minimum, certain key elements and considerations, including:

- Comprehensive Identification and Assessment of Risks – see above regarding types of risks;
- Relating Risk to Capital – considering the nature, scale and complexity of the FSP, determination of capital needs, setting internal targets, and integration with other business processes;
- Oversight – review of the policies, procedures, systems, controls and personnel for identifying, analysing, assessing, monitoring and measuring risk exposures;
- Monitoring and Reporting – processes that take into account the current and forecasted business environments and can be adjusted when appropriate, so that capital remains adequate during periods when the FSP is under stress and through entire business cycles; and
- Internal Controls and Objective Review – review of the internal control structure and regular reviews of the ORSA process for integrity, accuracy, and reasonableness.

There is no single correct approach to an ORSA, and one approach will not fit all FSPs. Therefore, these key elements and considerations are broadly stated and the manner with which some of these elements are integrated in an FSP's ORSA may vary by FSP.

6. Risk Appetite and Limits

6.1 Risk Appetite Framework

An FSP should develop a Risk Appetite Framework that takes into account its risk profile. It should be enterprise-wide and tailored to the FSP's business activities and operations. The board should ensure that the Risk Appetite Framework is reviewed regularly and updated to ensure that it remains appropriate relative to the risk profile of the FSP, its long-term strategic plan and its operating environment.

The Risk Appetite Framework, as approved by the board, should be well-understood throughout the organization and embedded within the culture of the FSP. All operational, financial and corporate policies, practices and procedures of the FSP should be guided by the Risk Appetite Framework.

The Risk Appetite Framework should set basic goals, benchmarks, parameters and limits (e.g., level of losses) as to the amount of risk the FSP is willing to accept, taking into account various financial, operational and macroeconomic factors. It should consider the material risks to the FSP, as well as the institution's reputation with its stakeholders.

The Risk Appetite Framework should be forward-looking and consistent with the FSP's business model, overall philosophy, short-term and long-term strategy and corresponding risk mitigation. It is intended to provide boundaries on the on-going operations of the FSP with respect to activities and participation in markets that are not consistent with the stated risk appetite.

The establishment of controls and a process to ensure their effectiveness are critical elements of the Risk Appetite Framework, as they help to ensure that the FSP stays within the risk boundaries set by the board.

The Risk Appetite Framework should contain a risk appetite statement and risk limits, as well as an outline of the roles and responsibilities of those overseeing the implementation of the Risk Appetite Framework. The Risk Appetite Framework is an integral part of the FSP's overall enterprise-risk management framework.

6.2 Risk Appetite Statement

The risk appetite statement reflects the aggregate level and type of risk that the FSP is willing to accept in order to achieve its business objectives. Key features of the risk appetite statement are:

- It should be linked to the FSP's short-term and long-term strategic, capital and financial plans, as well as compensation programs.
- It includes qualitative and quantitative measures that can be aggregated and disaggregated.

Qualitative measures may include:

- Significant risks the FSP wants to take and the reasons why;
- Significant risks the FSP wants to avoid and the reasons why;
- Attitude towards regulatory compliance; and
- Underlying assumptions and risks.

Quantitative measures may include measures of loss or negative events (such as earnings, capital or liquidity, earnings per share at risk or volatility) that the FSP is willing to accept.

- It should be forward-looking.
- It should consider normal and stressed scenarios.
- It should aim to be within the FSP's risk capacity (i.e., regulatory constraints).

6.3 Risk Limits

Risk limits are the allocation of the FSP's risk appetite statement to:

- Specific risk categories (e.g., credit, market, insurance, liquidity, operational);
- The business unit or platform level (e.g., retail, capital markets);
- Lines of business or product level (e.g., concentration limits); and
- More granular levels, as appropriate.

Risk limits are often expressed in quantitative terms, and are specific, measurable, frequency-based and reportable.

6.4 Relationship to Other Risk Management Strategies and Policies

Once approved by the board, the Risk Appetite Framework should be implemented by senior management throughout the organization as an integral part of the overall enterprise risk management framework of the FSP. The Risk Appetite Framework should align with the organization's strategy, its financial and capital plans, its business unit strategies and day-to-day operations, as well as its risk management policies (e.g., risk limits, risk selection/underwriting guidelines and criteria, lending policies, investment strategy and policies, reinsurance risk management policy, etc.) and compensation programs. An FSP would typically have risk management strategies and policies to deal with specific types of risks, in addition to the overall risk appetite statement[2]. Where the Risk Appetite Framework sets aggregate limits that will be shared among different units, the basis on which such limits will be shared should be clearly identified and communicated.

7. Risk Management Systems and Procedures

An FSP should establish appropriate systems and procedures to implement its risk management policies, which include risk identification, measurement, control, and monitoring mechanisms.

[2] For example, the Guidelines for Savings and Credit Cooperative Societies (November 2019), Risk-based Capital Adequacy Requirements, Defined Benefit Fund Funding Guideline, Insurance Core Principles (ICP) 8: Risk Management & Internal Controls, Insurance Core Principles (ICP) 16: Enterprise Risk Management, Basel Core Principles for effective Banking Supervision (BCP) 15: Risk Management Process, ISO 31000 Standard etc..

They should include clear mandates, an appropriate organisation structure, committees, sufficient resources for implementation, operational policies, procedures and systems, and reporting mechanisms.

7.1 Organisation

Senior management should have policies and practices to delegate responsibilities, including the responsibilities related to risk management, to members of operational management and to regularly review the appropriateness of the delegation. The mandates for operational management positions should clearly define lines of authority, responsibility and accountability and be widely communicated within the FSP.

The organisational structure should establish clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits, including risk limits. The documented organisational structure should reflect actual operating practices. Control functions, such as compliance, risk management, internal audit, actuarial and financial should be independent of the operational functions.

Operational committees might be used to execute the management of significant activities and related risks. For example, an FSP might establish an asset-liability management committee, with representatives from its investment division, product line managers, actuary, and head of risk management. If so, the committees' mandates should be clearly defined and communicated within the FSP.

7.2 Resources

An FSP should have adequate resources (e.g., people, tools, data) for fulfilling operational management's responsibilities, including those related to risk management. This should be supported by policies and practices to determine the required level of resources, qualifications and competencies of staff, and continuing professional development and training programs to enhance staff competencies. The FSP should also have policies and practices for the selection, appointment, retention and succession of operational management and staff.

7.3 Operational Policies, Procedures and Practices

An FSP should have operational policies, procedures and practices that are appropriate given the FSP's activities and related risks. They should:

- Be consistent with the FSP's strategic policies and practices
- Support the implementation of the Risk Appetite Framework

- Ensure compliance with applicable laws, regulations and guidelines
- Be documented and communicated
- Be consistent with the FSP's day-to-day business activities
- Be reviewed and updated to take into account changes in the operating environment, the business activities of the FSP, or the risk appetite of the FSP.

An FSP should have policies, procedures and practices to report information needed by operational management to control the day-to-day business activities and identify issues of potential concern. It should also have policies, procedures and practices to monitor and follow up on the resolution of the identified issues.

8. Monitoring and Reporting

8.1 Management Information Systems

An FSP should be able to identify and measure all material risk exposures. This should be supported by management information systems that provide the board and senior management with timely reports on the financial condition, operating performance, and risk exposure of the FSP, as well as with regular, timely and sufficiently detailed reports for operational management.

An FSP should have management information systems that are adequate (both under normal circumstances and in periods of stress) for measuring, assessing and reporting on exposures across all risk types, products and counterparties. The key assumptions, data sources, and procedures used in measuring and monitoring risk should be appropriate and adequately documented and tested for reliability on an on-going basis.

Where an FSP uses models to measure components of risk, the board and senior management should understand the limitations and uncertainties relating to the output of the models and the risk inherent in their use. They should also assess whether the model outputs appear reasonable as a reflection of the risks assumed. The FSP should perform regular and independent validation and testing of the models.

8.2 Operational Reports

An FSP should have policies, procedures and practices to report information needed by operational management to control the day-to-day business activities and identify issues of potential concern. The reports should identify the level of risks being assumed compared to the risk limits.

The FSP should review significant or frequent policy exceptions to determine the potential impact on its risk profile as well as the effectiveness of its policies and procedures.

The reporting mechanisms should also facilitate operational management's full, open and timely disclosure to and discussion with senior management on all significant issues.

8.3 Reporting to the Board and Senior Management

An FSP should have policies, procedures and practices to report information needed by the board and senior management. Reports should reflect the FSP's risk profile and capital and liquidity needs. They should be provided on a timely basis in a form suitable for their use.

Reports to the board and senior management should contain sufficient information to provide a clear understanding of the FSP's risk exposures and enable them to identify any adverse trends. Reports should be consistent with the FSP's activities, structured to monitor exposures and compliance with the risk appetite statement, including risk limits, and, as appropriate, compare actual versus expected performance.

There should be clear guidelines on the types of information to be reported to the board and senior management on a regular basis as well as when certain information should be communicated immediately.

9. Controls

9.1 Internal Controls System

A system of internal controls is critical to effective risk management and as such an FSP should ensure that it has adequate internal control processes in place to effectively implement the risk management program.

Internal controls refer to a control system within an organisation that helps to ensure the proper conduct of its business and affairs. Internal controls encompass the policies, processes, culture, tasks and other aspects of an FSP that support the achievement of the FSP's objectives. A sound internal controls system facilitates the efficiency of operations, contributes to effective risk management, assists compliance with applicable laws and regulations, and strengthens capacity to respond appropriately to business opportunities.

The internal controls system should be designed and operated to assist the board and senior management in the fulfilment of their respective responsibilities for oversight and management of the FSP. The internal controls system should provide reasonable assurance that the FSP is being operated consistently with the strategy and risk appetite set by the board, agreed business objectives, agreed policies, processes and procedures, and applicable laws, regulations and guidelines.

The internal controls system should deal with the following issues:

- The type and level of risks posed by the nature and scope of the FSP's activities;
- The organizational structure and lines of authority and responsibility for monitoring adherence to policies, procedures and risk tolerance limits;
- Financial, operational, and regulatory reporting; and
- The independence and objectivity of internal audit and other control review functions.

In order to ensure adequacy of the FSP's internal controls, the following should be observed:

- Internal controls and information systems should be adequately tested and reviewed;
- The coverage, procedures, findings, and responses to audits and review tests should be adequately documented; and
- Any material weaknesses identified within the internal controls system should be given appropriate and timely high-level attention, and management's actions to address material weaknesses should be objectively verified and reviewed.

9.2 Risk Management Function

An FSP should establish an independent risk management function that is commensurate to the size, nature and complexity of its operations. For smaller scale operations, the function’s responsibilities may be incorporated into a single senior position.

The risk management function should primarily be responsible for the development of the FSP’s risk management policies and procedures and ensuring compliance with the policies and procedures. In order to be effective, this function should be independent from the activities it oversees, and have the requisite authority, sufficient resources and ability to raise issues directly to the board or relevant board committees.

The tasks of the risk management function should include:

- Coordinating the risk management process amongst other business units of the FSP’s operations;

- Establishing policies, practices, risk tolerance limits and other risk control mechanisms for senior management and board approval;
- Developing risk assessment and measurement systems;
- Monitoring the FSP's position against risk tolerance limits;
- Identifying and analysing potential risks and the impact of losses to the FSP's operations;
- Developing risk responses to identified losses that include contingency and business continuity programmes;
- Assisting in instilling a risk-based culture within the FSP's operations;
- Providing advice on changes in regulatory, legal or market conditions that may impact the FSP's operations;
- Conducting regular stress testing and scenario analysis;
- Regularly reporting to senior management, key persons in control functions and the board on the FSP's risks;
- Providing risk management recommendations that assist in strategic planning, decision making and the budgeting process of the FSP; and
- Providing recommendations on potential risks and their exposures to the board and senior management.

9.3 Internal Audit Function

The internal audit function should provide independent oversight of the effectiveness of, and adherence to, the FSP's organizational and procedural controls. It should also oversee the effectiveness of, and adherence to, the FSP's compliance and risk management policies and practices.

An FSP's audit committee and board should review the effectiveness of internal audits and other control review activities on a regular basis. The following criteria should be considered in assessing the quality of the internal audit function's oversight of the effectiveness of, and adherence to, the FSP's organizational and procedural controls. The application and weighting of the individual criteria will depend on the nature, scope, complexity, and risk profile of the FSP and should be considered together with the internal audit performance, in assessing its overall effectiveness.

- Clarity of its objectives and enterprise-wide authority for its activities;
- Authority to carry out its responsibilities independently;
- Right of access to the FSP's records, information and personnel;
- Authority to express an opinion on the effectiveness of, and adherence to, the FSP's organizational and procedural controls;

- Authority to follow-up with management on actions taken in response to audit findings and recommendations;
- Appropriateness of the stature and authority of the function head within the organization for the function to be effective in fulfilling its mandate;
- Extent to which the function head has direct access to senior management and the board (or Audit Committee);
- Appropriateness of the function's organizational structure.
- Extent to which the function is independent of the activities that it audits and the day-to-day internal control processes;
- Level of resources necessary to carry out responsibilities;
- Qualifications and competencies of staff comprising the function;
- Sufficiency of the staff development programs;
- Continuing professional development programs to enhance staff competencies;
- Adequacy of the function's resources and appropriateness of its collective qualifications and competencies for executing its mandate;
- Adequacy of policies and practices to ensure that audit methodologies conform to generally accepted industry practices and current professional standards.
- Appropriateness of audit methodologies and practices to execute the function's mandate.
- Extent to which the function's audit methodology is risk-based and responds to changes in the FSP's risk profile;
- Adequacy of policies and practices to review audit cycles in response to changes in the FSP's environment and risk profile; and
- Extent to which the annual audit planning process clearly identifies audit objectives and scope of work.

9.4 Periodic Review of the Effectiveness of Internal Controls

An FSP should regularly review the market environment in which it operates, draw appropriate conclusions as to the risks posed and take appropriate actions to manage adverse impacts of the environment on the FSP's business.

As appropriate, an FSP should conduct quantitative and qualitative analyses, such as stress tests and scenario analysis, having regard to the size and complexity of the FSP and the nature of its risk exposures

The FSP should implement and communicate to relevant staff an escalation process for reporting on risk issues within established reporting cycles and outside of them for matters of particular urgency.

The risk management framework should include a "feedback loop" which allows the board and senior management to take necessary action in response to changes in the risk profile of the FSP. The feedback loop will also ensure that decisions made by the board and senior management are implemented and that their effects are monitored to determine whether they are in fact appropriate.