|  |
| --- |
| **GUIDANCE NOTES** |

**2019.07 SPB RISK MANAGEMENT (v.2)**

* The SPB contains Standards in the form of mandatory actions and rules which in turn, provide support and direction for formal policies.
* The actions and rules as contained in the SPB are therefore compulsory and must be enforced in order to be effective.
* All Procedures referred to in the SPB are detailed step by step instructions that must be followed in order to achieve the FSP’s mandate.
* It is necessary that the FSP has comprehensive and consistent documentation of the procedures that it is developing.
* The Best Practice Principles in the SPB are recommendations to the FSP only when specific standards do not apply and are not part of formal policy statements.
* The contents and format of this document are provided as an example only. It is the responsibility of the user to customise the document to the user’s specific needs, circumstances and applicable legislation.
* **Disclaimer:** This document is of a generic nature and was compiled taking relevant statutory requirements into consideration. This document is provided as a guideline only and any reliance the user places on this document will be at the user’s own risk. Moonstone accepts no liability for any damages suffered or losses incurred arising from the use of this document.

**TABLE OF CONTENTS**

1. [Compliance Risk Area 2](#_Toc523308345)
2. [Regulatory Framework 2](#_Toc523308346)
3. [Corresponding Document(s) 2](#_Toc523308347)
4. [Responsible Person(s) 2](#_Toc523308348)
5. [Standards 2](#_Toc523308349)
6. [Procedures 3](#_Toc523308350)

[6.1 Risk Management Procedure 3](#_Toc523308351)

[6.2 Risk Management Meetings 3](#_Toc523308352)

[6.3 Risk Identification Procedure 3](#_Toc523308353)

[6.3.1 Communication......................... 3](#_Toc523308354)

[6.3.2 Context......................... 4](#_Toc523308355)

[6.3.3 Risk Evaluation & Regulatory Risk Registers 4](#_Toc523308356)

[6.3.4 Impact & Likelihood Rating 4](#_Toc523308357)

[6.3.5 Risk Response: Risk Treatment Options 5](#_Toc523308359)

[6.3.6 Monitoring of Risks and Review of the Outcomes 6](#_Toc523308360)

[6.4 Review............................... 6](#_Toc523308361)

1. [Best Practice Principles 6](#_Toc523308362)

|  |
| --- |
| **STANDARDS, PROCEDURES & BEST PRACTICE PRINCIPLES** |

**2019.07 RISK MANAGEMENT (v.2)**

# COMPLIANCE RISK AREA

1. GRC Function & Control Measures

# REGULATORY FRAMEWORK

* Board Notice 194 of 2017 – Determination of Fit & Proper Requirements for Financial Service Providers;
* Board Notice 80 of 2003 – General Code of Conduct for Authorised Financial Services Providers and Representatives;
* Financial Intelligence Centre Act 38 of 2001;
* Financial Advisory and Intermediary Services Act 37 of 2002;
* Financial Sector Regulation Act 9 of 2017; and
* Board Notice 79 of 2003 – Code of Conduct for Administrative and Discretionary Financial Service Providers.

# CORRESPONDING DOCUMENT(S)

2018.08 Risk Management Policy (v.1);

2018.08 RRR – FAIS (General) (v.1);

2018.08 RRR – GCOC (v.1);

2018.08 RRR – FICA (v.1);

2018.08 RRR – FAIS (Fit & Proper) (v.1);

# 2019.07 RRR - Admin and Disc FSP's COC (v.1)

# RESPONSIBLE PERSON(S)

All Key Individuals, Representatives and Persons responsible for the internal risk management of the FSP.

# STANDARDS

Section 11 of the General Code of Conduct for Authorised Financial Services Providers and Representatives (“the General Code of Conduct”) states that a provider must –

* at all times have and effectively employ the resources, procedures and appropriate technological systems that can reasonably be expected to eliminate as far as reasonably possible;
* the risk that clients, product suppliers and other providers or representatives will suffer financial loss through theft, fraud, other dishonest acts, poor administration, negligence, professional misconduct or culpable omissions.

Section 12 of the General Code of Conduct states that a provider must –

* structure the internal control procedures concerned so as to provide reasonable assurance that –
	+ the relevant business can be carried on in an orderly and efficient manner;
	+ financial and other information used or provided by the provider will be reliable; and
	+ all applicable laws are complied with.

Section 37(2) of Board Notice 194 of 2017 states that the governance framework of an FSP must –

* include, but not limited to, effective and adequate systems of corporate governance, risk management (including conduct risk management and internal controls that includes
	+ risk management policies, procedures and systems, including
	+ effective procedures for risk assessment, which identify the risks relating to the FSP’s activities, processes and systems, and where appropriate, set the level of risk tolerated by the FSP;
	+ effective procedures and systems –
		- to ensure compliance by the FSP, its officers, employees, key individuals and representatives with the FAIS Act and other applicable laws, including the Financial Intelligence Centre Act, 2001 and other applicable anti-money laundering or terrorist financing legislation;
		- To ensure compliance with decisions and decision-making procedures at all levels of the FSP;
		- To detect any risk of failure by the FSP to comply with applicable legislation, and put in place measures and procedures to minimise such risk; and
		- Provide for corrective actions to be taken.

# PROCEDURES

## **RISK MANAGEMENT PROCEDURE**

* The organisation has established planning processes in each department.
* Embedded within the various planning processes is the consideration of potential risks that could arise, as well as potential responses to these risks.
* However, to help ensure that important risks are not overlooked, a rigorous and systematic approach to identifying and adequately managing risks at strategic, operational and project level is essential.
* At every quarterly management meeting, risk management should be raised.
* All staff members are required to be aware of risk management concepts and practices and must be able to utilise and demonstrate application of risk management principles within their areas of control.
* This responsibility is due to the fact that managers are well placed to identify risks in their own areas and to recommend suitable strategies for controlling the impact of those risks.

## **RISK MANAGEMENT MEETINGS**

* At each monthly management meeting, managers are required to prepare for the meeting by identifying and discussing any potential risks facing their department. This involves thinking through the sources of the risks, the potential hazards, the possible causes and potential remedies.
* The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is also important to identify the risks associated with not pursuing an opportunity.
* Managers should typically consider the following risks;
* Strategic risks;
* Operational risks;
* Financial risks;
* Reputational risks;
* Legal and Regulatory risks;
* Business disruption risks;
* Human resources: risks that could affect internal staff members or clients and the external public;
* Environmental risks

## **RISK IDENTIFICATION PROCEDURE**

## **Communication**

* In order to ensure that managers identify applicable risks appropriately, where applicable, managers are required to communicate and consult with key stakeholders regarding risk management processes, issues and initiatives.
* Staff must ensure that relevant stakeholders are consulted and informed of risk management activities. This can be done through means such as training, continuous professional development activities and circulating standard agenda items on team meetings, or surveys with candidates, where necessary.

## **Context**

* When evaluating and managing risks, managers are required to establish the applicable context, which involves setting boundaries around the depth and breadth of risk management efforts.
* This is to ensure that each department remains focused on relevant issues within the risk management framework so as to ensure the achievement of organisational objectives.
* The following should be taken into consideration when defining the applicable context:
* The external environment, which includes socio-economic factors, demographics, financial and environmental issues.
* Who the stakeholders are and what interests of theirs are implicated. Examples of stakeholders include, candidates, clients, the Regulator, employees, insurers, service providers and suppliers and volunteers.
* The organisation’s internal environment, including the organisation’s goals, objectives, business culture, risk tolerance, systems, processes and resources.

## **Risk Evaluation & Regulatory Risk Registers**

* Once risks have been identified and the applicable context has been determined, managers are required to assess and ‘diagnose’ the risk in accordance with the applicable regulatory risk register.
* Each regulatory sourcew has its own Regulatory Risk Register, and must be completed according to the specific Regulatory Risk Register.
* Risk evaluation involves comparing the level of risk found during the analysis process against the organisation’s known priorities and requirements.
* The table below, which sets out the Risk Rating Matrix of the FSP, must be used to evaluate risks in conjunction with the Impact and Likelihood Rating Tables in paragraph 6.3.4 below.

##

## **Impact & Likelihood Rating**

* The determining factors of Impact and Likelihood have a separate classification system, which must be applied prior to deciding what the impact rating of the relevant risk on the Risk Rating Matrix would be.
* The **Impact Rating** can be classified as follows:

## The **Likelihood Rating** can be classified as follows:

## **Risk Response: Risk Treatment Options**

* Risk treatment involves selecting one or more options for modifying risks and implementing those options.
* It furthermore involves identifying and evaluating existing controls and management systems to determine if further action is required.
* Existing controls are identified and then assessed according to their level of effectiveness. Managers are then required to develop a detailed strategy to manage and monitor the risk.
* For the various levels of risk, the following treatment strategies are required:
* For risks that fall within the **very high spectrum**, as indicated by the red blocks in the Risk Rating Matrix in paragraph 6.3.3 above, immediate action is required as it has the potential to cause significant damage to the organisation.
* For risks that fall within the **high spectrum**, as indicated by the orange blocks in the Risk Rating Matrix in paragraph 6.3.3 above, effective treatment is required through routine or specific procedures is required.
* For risks that fall within the **tolerable spectrum**, as indicated by the yellow blocks in the Risk Rating Matrix in paragraph 6.3.3 above, treatment is required through routine procedures.
* For risks that fall within the **low spectrum**, as indicated by the green blocks in the Risk Rating Matrix in paragraph 6.3.3 above, the department is required to continue to monitor and re-evaluate the risk and to ideally treat it with routine procedures if necessary.
* The treatment options are not necessarily mutually exclusive or appropriate in all circumstances.
* Risk treatment options can include the following:
* Avoidance: The risk can be avoided by deciding not to start or continue with the activity that gave rise to the risk;
* Taking or increasing the risk in order to pursue an opportunity;
* Removing the risk source;
* Changing the likelihood;
* Changing the consequences;
* Sharing the risk with another party or parties (including contracts, risk financing and insurance); and g) retaining the risk by informed decision.
* Management should include the following information when selecting a risk response:
* The reasons for selection of treatment options, including expected benefits to be gained;
* Those who are accountable for approving the plan and those responsible for implementing the plan;
* Proposed actions;
* Resource requirements including contingencies;
* Performance measures and constraints;
* Reporting and monitoring requirements; and
* Timing and schedule.

## **Monitoring of Risks and Review of the Outcomes**

* As risks rarely remain static, risks will be continuously monitored and reviewed and the effectiveness of the controls in place and of the risk treatment plans will be assessed.
* Feedback on the implementation and the effectiveness of the Risk Management Policy and Plan will be obtained from the risk reporting process, internal audits and other available information.
* Risks will be monitored regularly in line with their significance.
* At minimum, the risk register will be reviewed every six months.

## **REVIEW**

* On a bi-annual basis, management must provide assurance to the Governing Body that the risk management procedure has been integrated in the daily activities of the organisation.
* On a quarterly basis, the Chief Risk Officer (“the CRO”) must provide assurance to the governing body that the planned risk management activities are being implemented according to this risk management plan.
* This assurance shall be communicated to the governing body in the form of a report from the CRO.

# BEST PRACTICE PRINCIPLES

* None