

# Risk Management guide



|   |    |
|---|----|
| TABLE OF CONTENTS.....  | 1  |
| 1. INTRODUCTION: .....  | 2  |
| 2. ....   |    |
| 1.1 Acronyms/Abbreviations/Glossary.....                        | 2  |
| 1.2 General Code of Conduct.....                                | 2  |
| 1.3 Definitions .....   | 4  |
| 1.4 Risk Management Strategies .....                            | 5  |
| 1.5 Types of risks: .....                                       | 6  |
| 2. ETHICS AS A FOUNDATION FOR RISK MANAGEMENT.....              | 6  |
| 3. DEVELOPING A RISK MANAGEMENT PLAN:.....                      | 7  |
| 4. GENERAL HINTS FOR COMPILING YOUR RISK MANAGEMENT PLAN: ..... | 10 |
| 5. EXAMPLES OF RISK MANAGEMENT PLAN FORMATS: .....              | 11 |

# Risk Management guide



## 1. INTRODUCTION:

### 1.1 Acronyms/Abbreviations/Glossary

**FAIS** means Financial Advisory and Intermediary Services

**FICA** means Financial Intelligence Centre Act

**FSP** means Financial Services Provider

**RMP** means Risk Management Plan

**BN** means Board Notice

**GCOC** means General Code of Conduct

### 1.2 General Code of Conduct

Sections 11 to 13 of the General Code of Conduct for Authorised Financial Services Providers and their Representatives (“the General Code”) deal with a FSP’s responsibilities in respect of Risk Management.

**Section 11** of the General Code deals with the control measures required and provides 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 relates to the specific control measures required and provides that:

*“A provider, excluding a representative, must, without limiting the generality of section 11, structure the internal control procedures concerned so as to provide reasonable assurance that-*

# Risk Management guide



- (a) the relevant business can be carried on in an orderly and efficient manner;*
- (b) financial and other information used or provided by the provider will be reliable;*
- and*
- (c) all applicable laws are complied with.”*

**Section 13** of the General Code deals with Insurance and provides that:

*“A provider, excluding a representative, must, if, and to the extent, required by the registrar maintain in force suitable guarantees or professional indemnity or fidelity insurance cover.”*

From the abovementioned sections of the General Code it is evident that it is a necessity for a FSP to develop a Risk Management Plan.

# Risk Management guide



## 1.3 Definitions

| Term                   | Explanation   |
|------------------------|---|
| <b>Risk</b>            | A <b>risk</b> can be defined as the possibility of a negative occurrence such as damage, injury, liability, loss which is caused by either an internal or external vulnerability.   |
| <b>Risk Management</b> | <b>Risk Management</b> is the process of analysing and assessing your exposure to risk and determining how to best manage your exposure to limit or even eliminate the risks. Risk management involves the identification, assessment, prioritisation of the risks and the application of resources to minimise, monitor and control the probability and/or impact of the negative occurrences. |
| <b>Management</b>      | <b>Management</b> is leading or making things happen through people. It is also the use or co-ordination of the resources and people's responsibilities for directing or running an organisation.   |
| <b>Plan</b>            | A <b>plan</b> involves knowing where you are currently your FSP, where do you want your FSP to be in the future and how you are going to get there.   |
| <b>Inherent risks</b>  | <b>An inherent risk is those risks that</b> exist due to natural activities of the business. (Risks that are unavoidable)   |
| <b>Risk appetite</b>   | The level of risk that an organization is prepared to accept, before action is required necessary to reduce that particular risk.   |

# Risk Management guide



|                       |  |
|-----------------------|--|
| <b>Risk tolerance</b> | The ability of an organization to survive the losses associated with risks |
| <b>Risk register</b>  | A database of the risks that an organisation is exposed to.                |

## 1.4 Risk Management Strategies

Below are four potential risk response strategies for risk management:

| <b>Strategy</b>   | <b>Brief Description</b>  |
|-------------------|---|
| Accept the risk   | Simply taking a chance that the risk may or may not occur/happen      |
| Avoid the risk    | Changing your plans in order to prevent the risk from arising         |
| Mitigate the risk | Reducing/lessening the impact/seriousness of the risk and probability |
| Transfer the risk | Transferring the risk to a capable party that can manage the outcome  |

Risk management should:

- Create and/or add value to your FSP
- Form part of your FSP's processes
- Identify risks facing your organisation
- Be part of decision making within your FSP
- Specifically address uncertainty within your FSP
- Be systematic and structured (shouldn't be haphazard)
- Be based on the best available information
- Be tailored to suit your FSP
- Take into consideration human factors (including segregation of duties)
- Be transparent/realistic and include all the risks that your FSP faces
- Be able to be continuously improved and enhanced

# Risk Management guide



## 1.5 Types of Risks

There are different types of risks that can be applicable to your FSP. Examples of such risks are:

| <b>Types of Risks</b>       | <b>Brief Description</b>   |
|-----------------------------|--|
| Compliance Risk             | Non-conformance with stated requirements. At an FSP level conformance is achieved through management processes which identify the applicable requirements.                           |
| Financial Risk              | Non-conformance with multiple types of risks associated with financing, including financial transactions that include the FSP's loans which could face the risk of default payments. |
| Operational Risk            | Non-conformance with operational requirements arising from the FSP's business functions.   |
| Human Resources /Staff Risk | Non-conformance with fit and proper requirements in terms of Board Notice 106 of 2008.   |
| Litigation Risk             | Non-conformance with legal and regulatory requirements which may result in litigation against the FSP.   |
| Reputational Risk           | Non-conformance with the trustworthiness of the FSP.   |
| Market risk                 | <b>Market risk</b> refers to the potential for FSPs income(in value) to decrease due to factors affecting the entire market/industry   |

## ETHICS AS A FOUNDATION FOR RISK MANAGEMENT

The main reason behind regulatory supervision is to ensure the implementation of the specific legislation whereas the objective of legislation is to prescribe to people subject to the law how they should act.

From the above it follows that the object of the FAIS legislation is to prescribe the manner in which financial services should be rendered to members of the public. Ethical conduct of all FSPs will ensure that the risks within a FSP are lowered. When interacting with prospective clients and existing clients, FSPs should always act in good faith to the benefit of themselves and others.

# Risk Management guide



## 2. DEVELOPING A RISK MANAGEMENT PLAN

### Developing a Risk Management Plan

The following is an example of the steps that may be followed to assist an FSP to develop its own Risk Management Plan (RMP):

- Step 1:** Identify the specific risks to your FSP
- Step 2:** Analyse and evaluate the risks identified
- Step 3:** Determine how you will manage the risks
- Step 4:** Monitor and review the risks

The above steps are discussed in more detail below:

### **Step 1: Identify the specific risks to your FSP**

Think of all the risks that your FSP may be faced with. You should not limit risks to laws and regulations, for instance the risks of non-compliance with the FAIS and FICA legislation, but think of other risks such as computer crashes, building fire, extended leave for the key individual etc.

When identifying the risks that are specific to your FSP you need to ask yourself “what could happen”. Some of the areas that you can look at when identifying your risks are:

| <b>Risks</b>        | <b>Brief Description</b>  |
|---------------------|---|
| Business objectives | Consider your business objectives and what can threaten achieving these objectives  |
| Potential risks     | Identify/describe potential risks: This includes inherent risks and day to day risks preventing the achievement of business objectives. The potential causes of these risks should also be identified |
| Market              | Think of your competitors, loss of clients and income   |
| Staff               | Are the FSP's employees happy in their work place and does the FSP employ competent employees?  |
| Customer service    | Ensure that the FSP has the required procedures and controls in respect of complaints and the resolution of complaints  |

# Risk Management guide



|                      |  |
|----------------------|--|
| Legal issues         | The possibility of legal action against the FSP or Ombud's determination   |
| Insurance            | Does the FSP have Professional Indemnity Cover in terms of Board Notice 123 of 2008?<br>Is the FSP required to have IGF in terms of Section 45 of the Short-Term Insurance Act?                                      |
| Resources/Capacity   | Does the FSP have enough resources to conduct business and does the FSP satisfy the operational ability requirements contained in the Determination of Fit and Proper Requirements (Board Notice 106 of 2008)?       |
| Disaster             | What will happen if there were floods or the FSP's offices burnt down?   |
| Fraud                | Internal fraud committed by the FSP's employees and external fraud committed by the FSP's clients or product suppliers   |
| Data security        | Back-up of the FSP's systems, anti-virus software, maintaining the confidentiality of client information by using passwords and firewalls etc.   |
| Economic downturn    | What will happen if there is a recession and clients have less disposable income and may have to cancel policies or pay them up?   |
| Financial compliance | Ensure that the FSP has enough funds to conduct business in order to satisfy the statutory financial soundness requirements contained in the Determination of Fit and Proper Requirements (Board Notice 106 of 2008) |

## Step 2: Analyse and evaluate the risks identified

Prioritise the risks. When you prioritise risks you need to look at the impact/seriousness of the risk on your business and the probability of the risk that can actually occur/happen.

You need to have a thorough understanding of the risks identified, understand their causes and consequences. Ask yourself the following questions:

- How likely is it that the risk will occur/happen? Probability
- How bad will it be if the risk occurs/happens? Seriousness



# Risk Management guide



## **Step 3: Determine how you will manage the risks**

You should ask yourself the following questions:

- How will I reduce/eliminate the probability of the risk occurring/happening?
- How will I reduce/eliminate the impact/seriousness of the risk if it occurred/happened?

You should ask yourself the above questions for all the risks identified and your response to the questions should be your strategy for reducing or eliminating the risk. Your strategy should then be noted in your risk management plan.

## **Step 4: Monitor and review the risks**

You should review your risk management plan from time to time to avoid it becoming irrelevant and not reflective of actual potential risks. You may review your risks and risk management plan every year or as various situations arise.

# Risk Management guide



Risks can also be monitored and updated by using a risk register. (See example below)

| No | Risk  | Risk description   | Risk owner | Impact (H/M/L) | Impact Type   | Activity since last report  | Status (potential, active/closed) |
|----|---|--|------------|----------------|---|---|-----------------------------------|
| 1. | Non-compliance with the provisions of FAIS - specifically passing of regulatory Examinations. | Failure of compliance with the provisions of FAIS (passing of regulatory examination) resulting in potential financial loss, damage to reputation of SIS admin and potential debarment of key individuals. | Koketso    | H              | Reputational<br>Financial loss                        | All key individual registered for RE exams. Exams to be written on 30 June.   | Active                            |
| 2. | Inability of business to have adequate record keeping.  | Inability of business to have adequate record keeping including source documentation and audit trails resulting in a loss of income, fines and potential reputation damage.                                | Carol      | M              | Reputational<br>Operational<br>Business<br>Continuity | Record keeping system was upgraded. All communication with clients is recorded and can be traced. Two external servers in place for backup process. | Closed                            |
| 3. |   |  |            |                |   |   |                                   |

A risk management plan will prioritise the execution of the identified risks in order of impact.

Note that the risk management plan should always be current.

In reviewing the risks/plans the following can be considered:

- What are the risks (are they still potential threats) and how were they evaluated and controlled. Risk identification should be a continuous process as some risks may become irrelevant as mentioned above.
- The effectiveness of the risk management process. Has it worked for your business and has it helped to manage the risks.



## 4. GENERAL HINTS FOR COMPILING YOUR RISK MANAGEMENT PLAN:

- You must ensure that the risk management plan that you draw up is relevant to your business;
- If you make use of a template provided by someone else you must ensure that the risk management plan is customised to your own FSP and that you understand the content of the risk management plan;
- A risk management plan is a working document and should be reviewed;
- Think beyond the FAIS and FICA legislation and try to incorporate all risks that may be relevant to your FSP (what about the Close Corporations Act, Income Tax Act, Short Term insurance Act, Long Term insurance Act, National Credit Act, Labour Relations Act?);
- Don't be afraid to scrap something that you have included in your plan if you know that it isn't correct or appropriate to your business;
- Never risk more than you can afford to lose.

## 5. EXAMPLES OF RISK MANAGEMENT PLAN FORMATS:

We have included some examples of table formats which can be used when drawing up a risk management plan.

**It should be noted that these have only been provided to allow FSPs to have an idea of what a risk management plan can look like and they should not be seen as the template which must be used by FSP's.**

Table formats have been provided as it is easy to illustrate but should you wish to make use of a formal written document please feel free to do so:

An easy research tool for any person wishing to compile their own, personalized risk management plan is to make use of the internet.

# Risk Management guide



## Example 1:

| List of possible risks                  | Likelihood H/M/L | Impact H/M/L | What are we doing about it now                       | What more can we do about it   | Person responsible |
|---|------------------|--------------|--|--|--------------------|
| Record keeping: loss of paper documents | L                | H            | Documents stored in filing cabinets which are locked | Keeping scanned copies of documents & making weekly backups of electronic data | Admin              |

## Example 2:

| Risk identified   | Impact | Probability | Exposure | Control  | Review date          |
|---|--------|-------------|----------|----------|----------------------|
| FAIS Ombud determination where damages have to be paid to client. | High   | Low         | Medium   | PI cover | 31 December<br>..... |

## Example 3:

| Section of FAIS Act and subordinate legislation | Issue / risk  | Recommended Actions  | Risk Rating H / M / L | Responsible Person                      | Monitoring Frequency |
|---|---|--|-----------------------|---|----------------------|
| Sec 8: FAIS Payment of annual levies            | The FSP is required to pay annual levies in order for the FSP to continue to render financial services (furnish advice and / or render an intermediary service) | Ensure that levy invoice received is paid by the due date specified on invoice | High                  | Key individual / appointed staff member | Annually             |