TABLE OF CONTENTS

1. INTRODUCTION:

1.1 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-

(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.

1.2 Definitions

A **risk** 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.

Management 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 organization.

Risk management 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.

A **plan** involves knowing where your currently are with your FSP, where do you want your FSP to be in the future and how you are going to get there.

1.3 Risk Management Strategies

There are four potential strategies for risk management:

- Accept the risk- simply take the chance that the risk may or may not happen;
- Avoid risk - changing your plans in order to prevent the risk from arising;
- Mitigate risk- lessening the impact of the risk; and
- Transfer risk – transfer the risk to a capable party that can manage the outcome.

Risk management should:

- create value for your FSP;
- be an integral part of your FSPs processes;
- be part of decision making within your FSP;

- explicitly address uncertainty within your FSP;
- be systematic and structured;
- be based on the best available information ;
- be tailored to your FSP e.g. your risk management plan shouldn't be a standardised document that you obtained from another person / FSP and which you haven't customised to your own business;
- take into account human factors;
- be transparent and include all risks that your FSP faces; and
- be capable of continual improvement and enhancement.

1.4 Types of risks:

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

- Compliance risks;
- Financial risks;
- Operational risk;
- Human resources / staff risks
- Litigation risk; and
- Reputational risks

2. 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.

Integrity is a concept that is closely related to ethics, and it mainly refers to human character. A person is regarded as a person of integrity when they consistently adhere to a set of ethical standards. For this reason integrity is associated with concepts like fairness, consistency and uprightness.

3. DEVELOPING A RISK MANAGEMENT PLAN:

The following is an example of the steps that may be followed to assist a FSP in developing your own Risk Management Plan.

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**: Identifying specific risks to your FSP*

Brainstorm as many risks as you can think of for your FSP. You don't have to just list 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:

- Market – think of your competitors, loss of clients and income;
- Staff – are your employees happy in their work place and do you employ competent employees;
- Customer service – ensure that you have the required procedures and controls in respect of complaints and the resolution of complaints;
- Legal issues – think of the possibility legal action against you or even an Ombud's determination;

- Insurance – do you have PI cover or fidelity cover (Board Notice 123 of 2008)? Are you required to have IGF (Section 45 of the Short Term Insurance Act);
- Do you have sufficient resources to conduct business and do you satisfy the operational ability requirements contained in the Determination of Fit and proper Requirements (Board Notice 106 of 2008);
- Disaster – what would happen if there was a flood or your offices had to burn down;
- Fraud – internal fraud committed by employees and even external fraud committed by your clients or even product suppliers;
- Data security – back-ups of your systems, antivirus software, maintaining the confidentiality of client information by using passwords and firewalls etc;
- Economic downturn – E.g. what will happen in times of recession when your clients have less disposable income and may have to cancel policies or make them paid up?
- Financial compliance – ensuring sufficient funds to conduct business and whether you satisfy the statutory solvency requirements contained in the Determination of Fit and Proper Requirements (Board Notice 106 of 2008).

***Step 2**: Analyse and evaluate the risks identified*

This stage is characterised by the prioritisation of risks. When you prioritise risks you need to look at the impact of the risk on your business (the seriousness) and the probability of the risk actually occurring.

You need to thoroughly understand the risks identified, understand their causes and consequences. Ask yourself the following questions:

- How likely is it that the risk will occur ?(probability) ; and
- How bad will it be if the risk happens? (seriousness)

You can then rank the risks identified according to the probability or impact (your risk exposure) e.g. High risk, Medium risk, Low Risk or Most severe, moderately severs, minimal concern etc or you can even assign numerical scores to risk probability (l=low, 2=moderate and 3=high) and severity of impact (1=low, 2=moderate, 3=high). *A risk score would be the multiplication of the two scores.* Management's

attention would then be focused on those risks with a higher score and management will need to review them *to determine if the significant risks will be accepted, transferred (outsourced), or mitigated.*
You need to choose for yourself what rating system you want to use. Some people use colour for example red for high risk, orange for medium risk and yellow for low risks. The table below provides a guide on how you could determine your risk exposure:

Risk Exposure:	**Probability**			
Impact		**High**	**Medium**	**Low**
	High	**High**	**High**	**Medium**
	Medium	**High**	**Medium**	**Low**
	Low	**Medium**	**Low**	**Low**

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

The questions you should ask yourself here are:

- How will I reduce / eliminate the probability of the risk happening?; and
- How will I reduce / eliminate the impact of the risk if it had to happen?

Your will ask the above questions for all of the risk identified and your response to the questions would 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 your risks

You should perform periodic review of your risk management plan in order to avoid having the analysis become stale and not reflective of actual potential risks. You may review your risks and risk management plan on an annual basis or as various situations arise – the risk management plan should always be current.

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

- What the risks are (and if they are still potential threats) and how they were evaluated and controlled. Identification of risks should be a continuous process as some risks may become stale as mentioned above.

  For example, you may collect clients' short term insurance premiums and in a year or two's time decide to outsource the function to a premium collection facility. When you were collecting the short term insurance premiums, theft was going to be one the most potential risk that the FSP may have been faced with and that would have required the FSP to have AN IGF or other suitable guarantee in place. If you outsource this function then the IGF would no longer be necessary and you would need to update your risk management plan accordingly.

- The effectiveness of the process of risk management. 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 been 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.

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 assistant

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 ……

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