QUICKSURE

# RISK MANAGEMENT PLAN

# FOR

## QUICKSURE COMMERCIAL (PTY) LTD

FSP NO: 16903

VERSION :20260201

**TABLE OF CONTENTS**

| | |
|---|---|
| **FSP NAME:** | **Quicksure Commercial (Pty) Ltd** |
| **FSP NUMBER:** | **16903** |
| **RESPONSIBLE PERSON:** | **Andrea Hatton-Jones** |
| **COMPLIANCE OFFICER:** | **Adv. Daniel Opperman** |

| | |
|---|---|
| **REVIEW DATE:** | **1 February 2026** |
| **FULL NAME OF KEY INDIVIDUAL:** | **Andrea Hatton-Jones** |
| **SIGNATURE OF KEY INDIVIDUAL:** |  |

## ACRONYMS / ABBREVIATIONS

| | |
|---|---|
| **"FAIS" -** | **Financial Advisory and Intermediary Services** |
| **"FICA" -** | **Financial Intelligence Centre Act** |
| **"FSP" -** | **Financial Services Provider** |
| **"RMP" -** | **Risk Management Plan** |
| **"BN" -** | **Board Notice** |
| **"GCOC" -** | **General Code of Conduct** |
| **"POPI" -** | **Protection of Personal Information** |
| **"PAIA" -** | **Promotion of Access to Information Act** |

## GENERAL CODE OF CONDUCT (GCOC)

- According to the GCOC, an FSP needs to develop a Risk Management Plan.
- Sections 11 to 13 of the General Code of Conduct for Authorised Financial Services Providers and their Representatives ("the General Code") deal with the FSP's responsibilities concerning Risk Management.
- Section 11 of the GCOC 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 GCOC 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 with providing reasonable assurance that -*

  - *the relevant business can be carried out 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 13 of the GCOC 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."*

## DEFINITIONS

| | |
|---|---|
| **"Risk" -** | A risk can be defined as the possibility of a negative occurrence, such as damage, injury, liability, or loss, which is caused by either an internal or external vulnerability. |
| **"Risk Management" -** | 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, and prioritisation of risks and the application of resources to minimise, monitor, and control the probability and/or impact of negative occurrences. |
| **"Management" -** | Management is leading or making things happen through people. It is also the use or coordination of the resources and people's responsibilities for directing or running an organisation. |
| **"Plan" -** | A plan involves knowing where you are currently with your FSP, where you want your FSP to be in the future, and how you are going to get there. |
| **"Inherent risks" -** | An inherent risk is a risk that exists due to the natural activities of the business. (Unavoidable Risks). |
| **"Risk appetite" -** | The level of risk that an organization is prepared to accept before action is necessary to reduce that particular risk. |
| **"Risk tolerance" -** | The ability of an organization to survive the losses associated with risks |
| **"Risk Register" -** | A database of the risks that an organisation is exposed to. |

## POTENTIAL RISK RESPONSE STRATEGIES FOR RISK MANAGEMENT

| STRATEGY | DESCRIPTION |
|---|---|
| Accept the risk | Simply taking a chance that the risk may or may not occur/happen. |
| Avoid the risk | Change your plans 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 must:

- Create and add value to the FSP
- Form part of the FSP's processes
- Identify risks facing the FSP
- Be part of decision-making within the FSP
- Specifically address uncertainty within the FSP
- Be systematic and structured
- Be based on the best available information

- Be tailored to suit the FSP
- Take into consideration human factors (including segregation of duties)
- Be transparent/realistic and include all the risks that the FSP faces
- Be able to be continuously improved and enhanced

### TYPES OF RISKS

Different types of risks can apply to the FSP. Examples are:

| TYPES OF RISKS | DESCRIPTION |
|---|---|
| Compliance Risk | Non-compliance with stated requirements. At an FSP level, conformance is achieved through management processes that identify the applicable requirements. |
| Financial Risk | Non-compliance 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-compliance with operational requirements arising from the FSP's business functions. |
| Human Resources /Staff Risk | Non-compliance with fit and proper requirements in terms of Board Notice 106 of 2008. |
| Litigation Risk | Non-compliance with legal and regulatory requirements, which may result in litigation against the FSP. |
| Reputational Risk | Non-compliance with the honesty and integrity of the FSP. |
| Market risk | Market risk refers to the potential for the FSP's income (in value) to decrease due to factors affecting the entire market/Industry |

## 1. INTRODUCTION

**Quicksure Commercial (Pty) Ltd – FSP No: 16903**, renders financial services in the following classes of business:

- Short-term Insurance: Personal Lines
- Short-term Insurance: Commercial Lines

**Quicksure Commercial (Pty) Ltd's** Clientele includes individuals, professionals, businesses, and corporations.

**Quicksure Commercial (Pty) Ltd – FSP No: 16903** employs the resources, procedures, and appropriate systems that can be reasonably expected to eliminate 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.

**Quicksure Commercial (Pty) Ltd – FSP No: 16903** structures its internal control procedures to provide reasonable assurance that:

- The business can be carried on in an orderly and efficient manner.
- Financial and other information used or provided will be reliable;
- All applicable laws are complied with.

The Registrar requires all Authorised Financial Services Providers to have Professional Indemnity cover.

**Quicksure Commercial (Pty) Ltd – FSP No: 16903** currently has professional indemnity cover in place for R 20 000 000 (Twenty Million).

## 2. MAIN RISKS

### ELECTRONIC RECORD KEEPING

**2.1.** In terms of electronic information, **Quicksure Commercial (Pty) Ltd – FSP No: 16903** has suitable access

security in place. All PC's in the office can only be accessed via a password. Electronic information is backed up regularly.

### SECURITY

**2.2.** In terms of physical security of assets and data, access to offices is secure, and client files are locked away.

### FINANCIALS

**2.3.** **Quicksure Commercial (Pty) Ltd – FSP No: 16903** monitors banking statements, income, and expenses regularly.

### BUSINESS POLICIES

**2.4.** All business processes, policies, and controls are documented, viz contracts with product suppliers. Legislation applicable to **Quicksure Commercial (Pty) Ltd – FSP No: 16903** includes the following:

- Basic Conditions of Employment Act
- Companies Act
- Electronic Communications and Transactions Act
- Financial Advisory and Intermediary Services Act
- Financial Intelligence Centre Act
- Income Tax Act
- Labour Relations Act
- National Credit Act
- Occupational Health and Safety Act
- Prevention of Organized Crime Act
- Short-term Insurance Act
- Unemployment Insurance Act
- Promotion of Access to Information Act
- Protection of Personal Information Act
- Insurance Act

## 3. RESPONSIBLE PERSONS

**3.1.** **Andrea Tracey Hatton-Jones** is ultimately responsible and accountable for establishing and maintaining risk management systems.

**3.2.** Risk management is a team effort where key individuals and administrative personnel are included in the process to ensure effective control and mitigation of risks.

## 4. RISK AND CONTROL

**4.1.** A provider must implement a comprehensive system of controls to ensure that risks are reduced and that the objectives of the provider are achieved.

**4.2.** The control environment should include ethical values, the compliance culture of the provider, and the competence of all involved.

Essential aspects of control should include:

- the control environment;
- risk identification and evaluation;
- control activities;
- information and communication;
- monitoring and management.

**4.3.** Any risk must be identified and reported promptly through the control systems to improve the risk profile of the business.

**4.4.** The provider should consider the need for a confidential reporting process (whistle-blowing) that covers fraud and similar risks.

## 5. APPLICATION OF RISK MANAGEMENT

**5.1.** The key individual is responsible for establishing risk strategies and policies. The key individual must also review the effectiveness of these policies regularly to ensure that they will guide responsible persons in executing their duties.

**5.2.** In reviewing the policies and processes, the following should be considered:

- what the risks are and how they will be identified, evaluated, and controlled;
- the effectiveness of the process of risk management;
- whether steps are taken timeously to rectify defects;
- whether the review points to a need for more stringent

controls. Risks can be assessed according to the following criteria:

Type of risk;

- the seriousness of the impact it may have on the business and third parties;
- the probability that a risk may occur;

The above criteria can then be rated on a scale of high, medium, and

low. Types of risks:

- regulatory;
- operational;
- financial;
- reputation

### Steps in Developing a Risk Management Plan (RMP)

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

Specific risks should not be limited to laws and regulations, like the risk of non-compliance with the FAIS and FICA legislation, but must also include risks such as computer crashes, building fires, extended leave for the key individuals, etc. Some of the areas that the FSP must consider when identifying risks are:

| RISKS | DESCRIPTION |
|---|---|
| Business objectives | Consider the FSP's objectives and what can threaten the achievement of these objectives. |
| Potential risks | Identify/describe potential risks: This includes inherent risks and day-to-day risks preventing the achievement of the FSP's objectives. The potential causes of these risks should also be identified. |
| Market | Think of the FSP's competitors, loss of clients, and income. |
| Staff | Are the FSP's employees happy in their workplace, and does the FSP employ competent employees? |
| Customer service | Ensure that the FSP has the required procedures and controls concerning complaints and the resolution of complaints |
| Legal issues | The possibility of legal action against the FSP or the Ombud's determination |
| Insurance | Does the FSP have Professional Indemnity Cover in terms of Board Notice 123 of 2008? 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 in the case of flooding or if the FSP's offices are 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, and maintaining the confidentiality of the client information by using passwords, 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 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**

Risk must be prioritised. When prioritising risks, the FSP must look at the impact/seriousness of the risk on The FSP and the probability of the risk that can occur/happen. The FSP must have a thorough understanding of the risks identified and understand their causes and consequences. How likely is it that the risk will occur/happen? Probability

- How bad will it be if the risk occurs/happens? Seriousness

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

The following questions must be asked, and the response to these questions should be the strategy for reducing or eliminating the risk. The strategy should then be noted in your risk management plan.

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

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

The risk management plan should be reviewed from time to time to avoid it becoming irrelevant and not reflective of actual potential risks. The risks and risk management plan should be reviewed every year or as various situations arise.

The risk management plan is designed to prioritise the execution of the identified risks in order of impact.

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 the FSP, and has it helped to manage the FSP's risks?

| No | Risk | Risk Description | Risk Owner | Impact (High/ Medium/ Low) | Impact Type | Activity since the last report | Status (potential, active/ closed) |
|---|---|---|---|---|---|---|---|
| 1. | Non-compliance with the provisions of FAIS - specifically the passing of regulatory Examinations. | Failure to comply with the provisions of FAIS (passing the regulatory examination) results in potential financial loss, damage to reputation, and potential debarment of representatives. | Name of the responsible person | H | Reputational Financial Loss | Relevant representatives have booked to write the applicable RE exams. | Active |
| 2. | The inability of businesses to have adequate record-keeping. | The inability of businesses to have adequate record keeping, including source documentation and audit trails, results in a loss of income, fines, and potential reputation damage. | Name of the responsible person | M | Reputational Operational<br><br>Business Continuity | The record-keeping system was upgraded. All communication with clients is recorded and can be traced. Two external servers are in place for the backup process. | Closed |
| 3. | Death/illness/immigration of a key individual, thereby ending the continuance of the FSP. | The inability of FSP to operate without a key individual | Name of the responsible person | M | | Put succession planning in place by:<br>- Transition to a Private Company<br>- Recruit a successor<br>- Agreement with an existing attorn | Active |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | ey | |

## 6. MONITORING

**Andrea Tracey Hatton-Jones** monitors the risk management plan continuously.

**National Compliance** assists in monitoring and reporting to the FSP and the Financial Sector Conduct Authority (FSCA) in terms of legislation.

In the monitoring process, the following can be considered:

**6.1.** interviews with providers, key individuals, and personnel;

**6.2.** availability of relevant legislation;

**6.3.** evaluating complaints received and solutions offered;

**6.4.** inspection of relevant documentation and registers;

**6.5.** evaluating client files and records in respect of advice and solutions;

**6.6.** evaluating procedures followed when interacting with clients;

**6.7.** observing processes followed in rendering advice;

**6.8.** evaluating intermediary services rendered;

**6.9.** assist with the submission of financial statements;

**6.10.** assessing queries received from regulators.

Any risk must be identified and reported promptly through the control systems to improve the risk profile of the business.

## 7. REPORTING ON RISK MANAGEMENT POLICIES

The key individual may be requested by regulators to report on how they deal with risk

management. The following may need to be disclosed by the key individual:

**7.1.** that the key individual is responsible for the process of risk management, the system of internal control, and communication throughout the business;

**7.2.** that the system is regularly reviewed for effectiveness;

**7.3.** that there is a continuous process for identification, evaluation, and management of risks;

**7.4.** that there is an appropriate system of internal control to reduce risks to an acceptable level;

**7.5.** that provision is made for the FSP to continue its business activities in case of a serious risk impacting the business;

**7.6.** that the process is documented.

## 8. SUMMARY:

The implementation of the risk management plan ensures the following:

**8.1.** Identify risks early and continuously;

**8.2.** Thoroughly understand risks, their causes, and consequences;

**8.3.** Determine how to best avoid or reduce risks;

**8.4.** Establish internal controls to mitigate risks;

**8.5.** Monitor control systems and ensure timely and accurate reporting.