ARTICLE

FIC Guidance

Interpreting Draft FIC Guidance Note 7A and Draft Public Compliance Communication 114

The Financial Intelligence Centre (FIC) exists to apply measures outlined in the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), which are intended to make the financial system intolerant to abuse. The FIC does this by working towards fulfilling its mandate of assisting in identifying the proceeds of crime, combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction.[1]

The Financial Intelligence Centre (FIC) has called for comments from accountable and reporting institutions, supervisory bodies and other persons on the draft Guidance Note 7A (draft GN7A) Chapter 4 and draft Public Compliance Communication 114 (draft PCC 114).

This article serves as an interpretive note to both the above documents providing some insight as to the expectation of the FIC based on the current draft documents. Both of these documents will still need to be finalised once comments have been received.

The amendments in Draft GN7A relate only to Chapter 4 regarding the aspect relating to the Risk Management and Compliance Program (RMCP).

It must be noted that PCC 114 is applicable to Designated Non-Financial Businesses and Professions (DNFBP) and not to larger Accountable Institutions (AI's) having advanced compliance structures. However, the principles contained in the PCC may be applied and expanded upon by larger AI's.

[1] https://www.fic.gov.za/aboutus/Pages/WhoWeAre.aspx
https://www.fic.gov.za/

Don’t get confused by the terminology

It is important not to get confused with the terminology. For purposes of this article, the terminology used and their meanings are as follows:

Risk Based Approach
The approach followed in implementing controls which are based on the ML/TF/PF risk having been assessed (the approach is not a one size fits all).

Overall Risk Management and Compliance Programme (RMCP)
This is the overall programme which is designed to address the identified ML/TF/PF risks of the AI/enterprise and consists of, amongst others, policies, minimum standards, operating procedures, technology, structures and controls. The overall RMCP describes in detail how the AI/enterprise identifies, assesses, mitigates/manages, and monitors the ML/TF/PF risk.

Apex RMCP
This is a consolidated document explaining or summarising how the overall RMCP (the programme) is implemented and what elements contribute to the overall programme. The Apex document is NOT the programme, but merely a description of the programme referring to other documents forming part of the overall RMCP. This is the document approved by the Board and provided to either the Supervisor or Regulator when requested.

Client level risk assessments
This refers to the risk associated with a client relationship which is determined at the time of onboarding, and thereafter throughout the relationship the client has with the AI/enterprise. This risk is determined by assessing all the risk factors as described above for each client.

Enterprise-wide Risk Assessment (also referred to as a Business Risk Assessment)

An assessment which determines the inherent risks of the enterprise, an assessment of the controls to address the identified risk, resulting in the overall residual risk of the enterprise. Where an enterprise or AI has a number of accountable institutions being part of the overall group or enterprise, each one of the AI's would perform a business risk assessment with the sum of all the business risk assessment rolling up in an enterprise-wide risk assessment. This assessment is performed on an ongoing basis and such assessments should be re-performed on an annual to 18-month basis, or when circumstances dictate that it should be re-performed. The performance of such an assessment and the outcome thereof must be evidenced.

Risk factor assessments

Risk factor assessments – these are assessments of various risk factors which feed into both the enterprise-wide risk assessment, as well as the customer risk assessment, and are factors associated with:

	**Client type risk** - Risk associated with the type of client being onboarded
	**Product risk** - Risk associated with the type of product the client wishes to have
	**Channel risk** - The risk associated with the manner in which the client was onboarded (the manner in which the client transacts may also be considered, especially for ongoing risk assessment of the client relationship)
	**Occupational/Industry risk** - The risk associated with a specific industry or occupation
	**Jurisdictional risk** - Risk associated with the jurisdiction of the client and jurisdictions with which the client transacts
	**Other risk types** - Any other risk type which the enterprise deems appropriate

These risk assessments form a vital part of the AI's/enterprise's overall risk assessment landscape and need to be re-assessed on an ongoing basis to ensure that the assessments are current.

The Apex RMCP Document and overall RMCP

In terms of the requirements set out in section 42 of the FIC Act, Accountable Institutions (AI's) must develop, document, maintain and implement a RMCP for anti-money laundering, combatting the financing of terrorism and counter proliferation financing (AML/CTF/CPF).

A RMCP is an **all-encompassing programme consisting of, amongst others (in relation to AML/CTF/CPF):**

- Policies
- Governance structures
- ML/TF/PF risk assessment of the AI
- Risk Factor assessments including new product assessments
- Methodologies and frameworks
- Minimum standards covering a number of aspects such as:
  - Customer Due Diligence (including Enhanced Due Diligence and Ongoing Due Diligence)
  - Customer screening (for Targeted Financial Sanctions, Politically Exposed Persons, Adverse Media and Private Lists)
  - Customer Risk Rating
  - Transaction Screening and Payment transparency
  - Transaction Monitoring and Regulatory Reporting
  - Risk Based Training
  - Customer Exits
  - Record Keeping
- Operating procedures supporting the above
- Target Operating Models to give effect to the AI's obligations and to manage the ML/TF/PF risk
- Technology applications used to manage the ML/TF/PF risk
- Organisational structure supporting the overall RMCP
- Management Information and the reporting of the effectiveness of the RMCP

As one can see from the supporting list, the RMCP (as a programme) contains numerous elements, and to try and incorporate this all into one RMCP document is challenging and could be quite complex from a single document perspective.

The most practical way to document the RMCP will be through an Apex RMCP document, which is supported and advocated by GN7A, as well as PCC 114.

Apex RMCP document

In essence a document describing or summarising the enterprise's overall programme without containing all the detail. Detail will be covered in the appropriate supporting documentation to the Apex RMCP document and will form part of the overall RMCP programme itself. The Apex RMCP document is the document that the Board of Directors will consider and approve with the various governance structures implemented by the Board and Senior Management giving effect to the elements of the overall RMCP (as described in the Apex RMCP document).

It cannot be expected by the Board to read and approve each and every document forming part of the overall RMCP of the enterprise/AI.

The Board exercises this obligation by way of approving the Apex RMCP document and delegating powers to the appropriate governance structures and senior management to document and approve other RMCP-related documents.

The Board will gain comfort as to the effectiveness of its overall RMCP through receiving appropriate reports from the various governance structures mandated to have oversight over the management of ML/TF/PF risk.

It is through this manner that the Board will demonstrate its responsibility for ensuring that the AI/enterprise maintains an effective AML/CTF/CPF control structure (through the overall RMCP).

By not receiving appropriate reports (applicable management information), the Board will not be in a position to demonstrate that it is fully engaged in taking ownership of the risk-based measures implemented by the AI/enterprise.

Failure to produce such an Apex RMCP document could be considered as inadequate documentation describing the accountable institution' RMCP as read with section 42(3) of the FIC Act, and thus AI's/enterprises are advised to review their current RMCP to ensure it complies with the requirements as set out in GN7A.

The Apex RMCP document can also be used to provide training to employees ensuring they understand how AML/CTF/CPF is approached by the enterprise/AI, with further detailed training being provided on role related matters of the various employees.

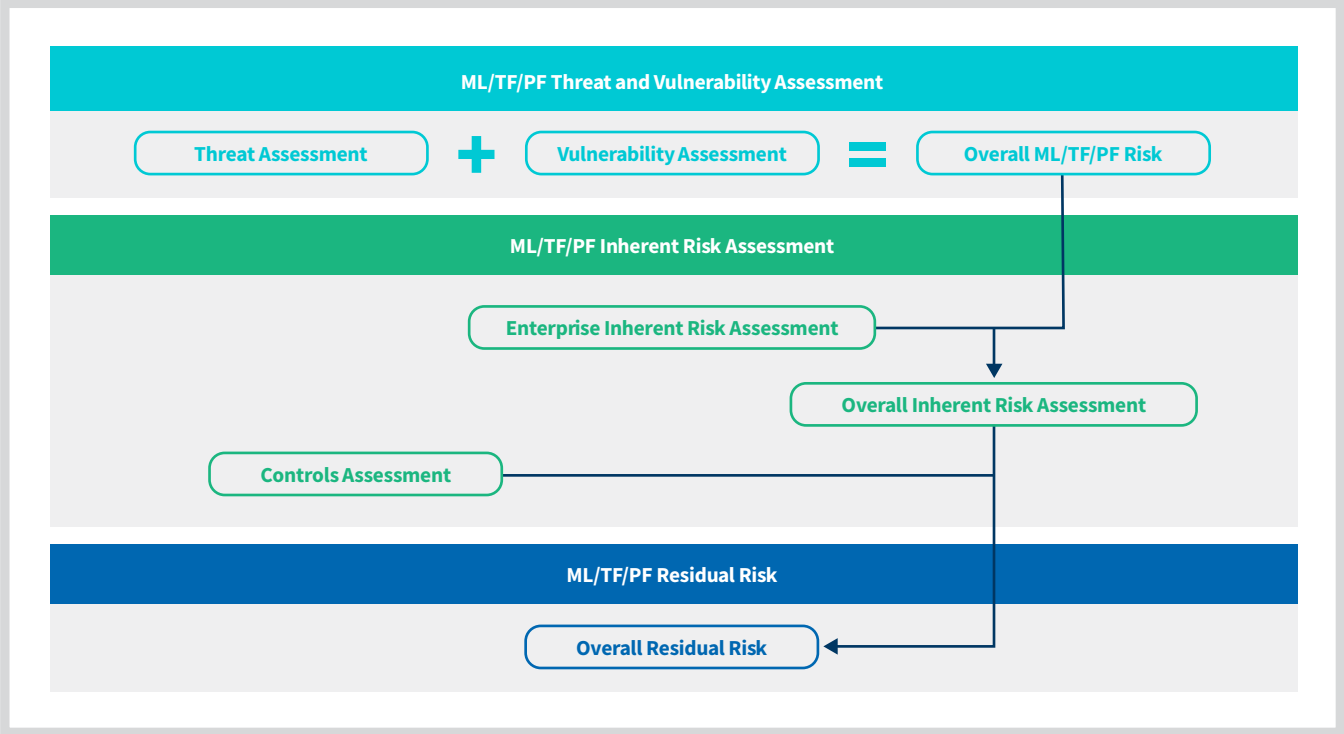
Pre-requisite for the design of the overall RMCP

A pre-requisite for the AI's/enterprise's overall RMCP (and thus its Apex RMCP document summarising the programme) is the performance of an enterprise-wide ML/TF/PF risk assessment (also sometimes referred to as a business risk assessment).

Such an assessment would be required to follow a specific methodology (which has been documented and approved) to demonstrate that the AI/enterprise clearly understands (in respect of ML/TF/PF):

- The threat and vulnerabilities it faces
- It's inherent risk
- How well its controls are performing in mitigating the identified inherent risk
- It's overall residual risk

The enterprise-wide risk assessment forms the basis, and is part of, the AI's/enterprise's overall RMCP and has specific impact on the mitigating controls of the AI/enterprise. Such an assessment will need to be performed on an annual to 18-month period and be clearly documented, with the outcome thereof being presented to the various governance structures and to the Board.



The content of the overall RMCP

There is no required format of an overall RMCP, however, the programme itself should cover the following aspects, which may be covered in various RMCP-related documentation, and also referenced in the Apex RMCP document:

The Governance and Oversight of AML/CTF/CPF - this includes:

- The overall governance structure for AML/CTF/CPF from the Board downwards
- Roles and responsibilities of the key governance structures as well as key functions/stakeholders/senior persons
- Appointment of the senior person as per section 42A of FICA
- The document hierarchy giving effect to the overall RMCP
- Governance and approval of the RMCP (including ongoing reviews and approval)
- Registration of AI's, Compliance Officer and Money Laundering Reporting Officers on goAML

Identifying and Assessing Risk

- The Risk Based Approach – how and to what it is applied
  - *Risk factors and their assessments*
  - *Customer Risk Assessment approach/methodology*
  - *Enterprise-wide Risk Assessment approach/methodology*
- The Enterprise-wide Risk Assessment and the Results
  - *Threat and vulnerability assessment*
  - *Inherent risk assessment*
  - *Controls assessment*
  - *Overall residual risk assessment*

Risk Mitigation (Controls)

- Risk Appetite statement
- Risk tolerance
- Policies, Standards, Procedures and Key Controls Framework (which include):
  - *Customer Due Diligence*
  - *Customer Screening*
  - *Customer Risk Assessment*
  - *Transaction Monitoring, screening and transparency*
  - *Ongoing Monitoring (due diligence, screening, risk rating etc…)*
  - *Management of Politically Exposed Persons/other specific customer types*
  - *Reporting obligations*
  - *Customer exits*
- Targeted Financial Sanctions – Terrorist and Proliferation Financing
- Training

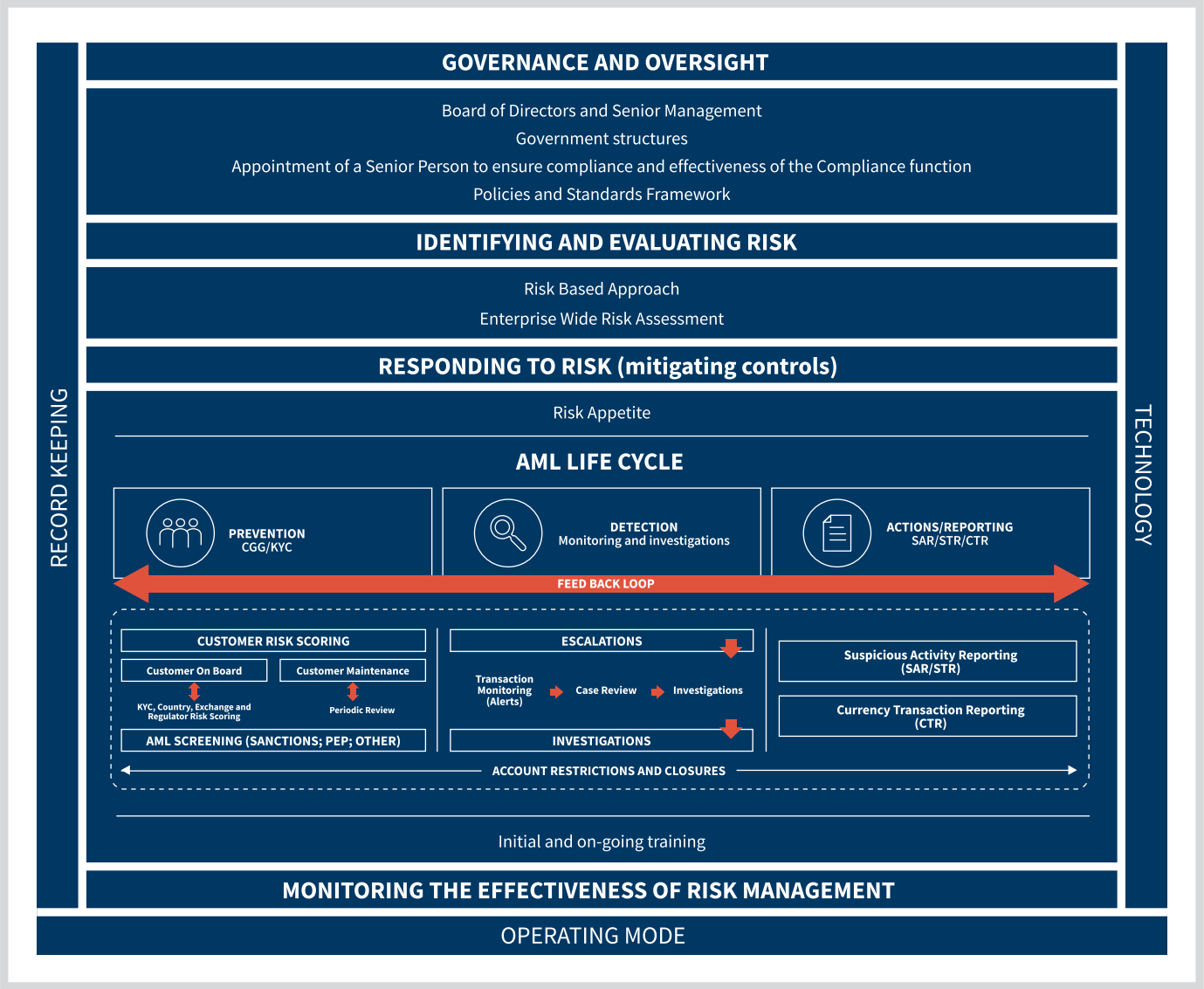
Risk Monitoring

- Key Indicators and Key Risk Indicators
- Management Information reports
- Escalation of non-compliance matters

Record keeping

Operating model for AML/CTF/CPF

Technology solutions used for AML/CTF/CPF



The above is used to draft the Apex RMCP document. Where a DNFBP entity is small in size and not that complex, there may be a case for having one RMCP document which covers some of the procedural aspects as well (PCC 114 provides such an example), however, one must be cautious not to follow a compliance mentality when doing so, but to rather focus on addressing the ML/TF/PF risk.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

KEVIN WEST
Senior Managing Director
Forensic Litigation Consulting
kevin.west@fticonsulting.com