NAVIGATE COMPLIANCE

COMPLIANCE RE-IMAGINED

Financial Services Compliance Guide

www.navigatecompliance.io | January 2026

Applicable to: Banks, Insurers, Investment Managers, and Financial Services Providers
Primary Regulators: Financial Intelligence Centre (FIC), Financial Sector Conduct Authority (FSCA), Prudential Authority (PA), Information Regulator

Purpose & Scope

This guide summarises the core compliance obligations for financial institutions operating in South Africa.

It focuses on four key frameworks — **Anti-Money Laundering (AML), Market Conduct, Cybersecurity, and Data Protection** — as well as the **FSCA OMNI Conduct and Risk Return** reporting requirements.

2. AML Compliance Obligations (FIC Act)

Objective: To prevent and detect money laundering, terrorist financing, and proliferation financing.

1. **Register with the Financial Intelligence Centre (FIC)** via goAML.
2. **Appoint a Compliance Officer** with sufficient seniority and competence.
3. **Develop and Implement a Risk Management and Compliance Programme (RMCP)** addressing client risk, product risk, geography, and delivery channels.
4. **Conduct Customer Due Diligence (CDD)** before entering any business relationship or executing a transaction.
5. **Apply Enhanced Due Diligence (EDD)** for higher-risk clients (e.g. PEPs, FPEPs, DPEPs).
6. **Undertake Ongoing Monitoring and Sanctions Screening** for all clients and relationships.
7. **Submit Regulatory Reports:**
   A. Cash Threshold Report (CTR) – > R49 999.99.
   B. Suspicious or Unusual Transaction/Activity Reports (STRs/SARs).
   C. Terrorist Property Reports (TPRs).
8. **Retain Records** for at least five years from the date of the last transaction or relationship termination.
9. **Provide AML Training and Employee Screening** in line with Directive 8.
10. **Submit FIC Risk & Compliance Returns (RCR)** annually per Directives 6 and 7.

Regulatory Focus Areas for 2026: Implementation of the RMCP.

3. Conduct Compliance (FSCA / COFI Framework)

Objective: To ensure that financial institutions treat customers fairly, manage conflicts of interest, and deliver sustainable outcomes.

Core Requirements:

1. **Treat Customers Fairly (TCF)**: Embed the six fairness outcomes into business models.
2. **Governance and Culture:**
   A. Board accountability for conduct risk.
   B. Fit and Proper oversight for key individuals and representatives.
3. **Product Governance:** Ensure product design, pricing, and distribution align with customer needs.
4. **Disclosure and Transparency:** Provide clear information on product features, risks, and fees.
5. **Complaints Management:** Maintain a documented, accessible complaints process with defined resolution timelines.
6. **Conflict of Interest Management:** Maintain registers, mitigation measures, and policy disclosure.
7. **Remuneration and Incentive Controls:** Prevent reward structures that encourage unfair outcomes.
8. **Reporting to the FSCA:** Submit the **OMNI Conduct of Business and Risk Return** on time and accurately.

COFI Readiness Checklist

Purpose:

- To assess your organisation's readiness for the Conduct of Financial Institutions Act (COFI) implementation by reviewing governance, culture, product governance, reporting, and client outcomes.

Regulator:

- Financial Sector Conduct Authority (FSCA)

Scope:

- All licensed financial institutions, FSPs, insurers, asset managers, banks, and service providers subject to market conduct regulation.

1. Governance and Accountability

Requirement	Description	Status
1.1 Board accountability for conduct	The board has approved a conduct strategy and policy that aligns with COFI outcomes.	☐
1.2 Governance structure	Roles and responsibilities for conduct risk management are formally assigned (Board, EXCO, Compliance, Risk).	☐
1.3 Conduct oversight function	A designated Conduct Officer or Committee oversees customer fairness and compliance culture.	☐
1.4 Integration with risk governance	Conduct risk is embedded in the enterprise risk management framework.	☐
1.5 Fit and proper governance	Senior management meet honesty, competence, and financial soundness requirements.	☐

2. Culture and Ethics

Requirement	Description	Status
2.1 Conduct culture framework	The organisation promotes integrity, transparency, and accountability at all levels.	☐
2.2 Tone from the top	Leaders demonstrate ethical conduct and reinforce "doing the right thing" over sales outcomes.	☐
2.3 Whistle-blowing mechanisms	Confidential channels for reporting misconduct exist and are accessible.	☐
2.4 Incentive and remuneration alignment	Variable pay does not encourage mis-selling or unfair treatment.	☐
2.5 Staff training and awareness	All staff receive conduct and ethics training annually.	☐

COFI Readiness Checklist

3. Product Design and Distribution

Requirement	Description	Status
3.1 Product governance framework	Policies define product design, approval, review, and discontinuation processes.	☐
3.2 Target market identification	Each product has a clearly defined and documented target market.	☐
3.3 Fair value assessment	Products are priced fairly, offering value to customers over time.	☐
3.4 Distribution controls	Sales channels are authorised, trained, and monitored for compliance.	☐
3.5 Product disclosure	Marketing material and contracts are clear, balanced, and in plain language.	☐

4. Customer Experience and Fair Outcomes

Requirement	Description	Status
4.1 Customer journey mapping	The organisation has mapped key customer touchpoints and identified conduct risks.	☐
4.2 TCF outcomes embedded	All six Treating Customers Fairly (TCF) outcomes are operationalised and monitored.	☐
4.3 Complaints management	A written, accessible complaints-handling process exists with defined turnaround times.	☐
4.4 Customer feedback integration	Feedback and complaints inform product and process improvements.	☐
4.5 Vulnerable customer policy	Procedures exist to identify and support vulnerable or high-risk customers.	☐

COFI Readiness Checklist

5. Systems, Controls, and Data

Requirement	Description	Status
5.1 Conduct data and MI reporting	Management Information (MI) dashboards include conduct KPIs (complaints, cancellations, claims turnaround, etc.).	☐
5.2 Integration with OMNI Return	Conduct data is mapped and ready for FSCA Omni Return reporting.	☐
5.3 Technology and cyber resilience	Systems support secure, reliable, and fair customer interactions (align with FSCA/PA Joint Standard 2024).	☐
5.4 Recordkeeping	Customer communications, advice, and disclosure records are securely stored and retrievable.	☐
5.5 Data protection and POPIA compliance	Customer information is processed lawfully and securely.	☐

6. Intermediaries, Agents, and Third Parties

Requirement	Description	Status
6.1 Third-party governance policy	Framework in place to oversee and manage agents, brokers, and outsourced partners.	☐
6.2 Due diligence	Onboarding and monitoring processes for intermediaries include conduct risk checks.	☐
6.3 SLA alignment	Service level agreements include COFI-aligned conduct and customer fairness clauses.	☐
6.4 Oversight and assurance	Periodic monitoring and review of intermediary compliance performance.	☐
6.5 Termination controls	Clear triggers and processes for ending relationships with non-compliant partners.	☐

7. Reporting, Monitoring, and Assurance

Requirement	Description	Status
7.1 Conduct MI dashboards	Reports presented to the Board and FSCA as part of ongoing supervision.	☐
7.2 Independent assurance	Internal Audit or external assurance reviews conduct governance annually.	☐

COFI Readiness Checklist

7. Reporting, Monitoring, and Assurance

Requirement	Description	Status
7.3 Self-assessment	Regular conduct self-assessments completed and documented.	☐
7.4 Regulatory reporting readiness	All required data fields and supporting evidence packs available for FSCA submissions.	☐
7.5 Continuous improvement	Findings and root causes from conduct incidents feed into remediation plans.	☐

8. Training, Competence, and Fit & Proper

Requirement	Description	Status
8.1 Fit and proper register	Maintained for all representatives, key individuals, and responsible persons.	☐
8.2 Competence framework	Defines minimum qualifications, ongoing CPD, and technical skills.	☐
8.3 Conduct and ethics training	Conduct training is included in onboarding and annual refreshers.	☐
8.4 Product and advice competence	Advisors are certified and authorised for the products they sell.	☐
8.5 Culture measurement	Employee surveys or scorecards used to assess conduct culture maturity.	☐

9. Transition and Implementation Planning

9.1 Gap analysis conducted	Organisation completed a COFI gap assessment against draft framework.	☐
9.2 Implementation roadmap	COFI transition plan with timelines and responsible owners documented.	☐
9.3 Policy alignment	Existing policies (FAIS, TCF, Treat Customers Fairly) mapped to COFI equivalents.	☐
9.4 Regulatory engagement	Management aware of FSCA guidance notes, workshops, and communication updates.	☐
9.5 Change management	Internal awareness campaigns conducted to prepare staff for COFI adoption.	☐

COFI Readiness Checklist

10. Summary and Readiness Score

Category	Maximum Score Achieved
Category	10
Governance & Culture	10
Product & Distribution	10
Customer Outcomes	10
Systems & Data	10
Intermediaries & Third Parties	10
Reporting & Assurance	10
Training & Fit & Proper	10
Transition Planning	80
Total Readiness (%)	***80%***

_____%

Scoring Guidance:

✅ 8–10 = Mature readiness

⚙️ 5–7 = Partial compliance, improvement needed

⚠️ 0–4 = Significant gaps, urgent remediation required

Key Takeaways

- **COFI consolidates market conduct regulation under one unified framework.**
- **Institutions must demonstrate proactive governance, customer fairness, and transparent data reporting.**
- **The FSCA OMNI Return will become the central monitoring tool for COFI conduct metrics.**
- **Embedding conduct into strategy, culture, and product design is the foundation of readiness.**

4. FSCA OMNI Conduct and Risk Return

Objective: To enable the FSCA to assess conduct, operational, and prudential risks across the financial sector.

Overview

- Introduced by the FSCA as a **single integrated return** consolidating multiple reports.
- Submitted via the **FSCA's E-portal (Regulatory Reporting System)**.
- Applies to **Category I–IV FSPs, insurers, banks, and retirement funds**.
- Data informs the FSCA's **risk-based supervisory approach** and future COFI implementation.

Key Components

A. **Governance and Compliance** – Fit and proper status, compliance monitoring, RMCP integration.
B. **Conduct and Customer Outcomes** – Complaints, product design, distribution oversight.
C. **Operational Risk and IT Governance** – Cyber incidents, business continuity, vendor risk.
D. **AML and Financial Crime Controls** – FIC reporting, screening, training, and RMCP alignment.
E. **Market Integrity Metrics** – Conflicts of interest, insider trading prevention, ethical conduct indicators.

Reporting Frequency and Timeline

- **Annual submission,** generally aligned with the institution's financial year-end.
- **Due dates:** Published in FSCA Communication 21 of 2023 and subsequent notices.
- **Responsible persons:** Key Individual and Compliance Officer must attest to the accuracy and completeness of the return.

Best Practices for Compliance

- Maintain **evidence packs** for each data field (e.g., training logs, board minutes, client complaints).
- Use **internal dashboards** to track conduct metrics quarterly.
- Perform **pre-submission assurance** (compliance review or internal audit sign-off).
- Retain copies of submissions and supporting records for at least five years.

5. Cybersecurity and Technology Risk (PA & FSCA Joint Standard 2024)

Objective: To ensure operational resilience and protection of financial systems.

Core Requirements:

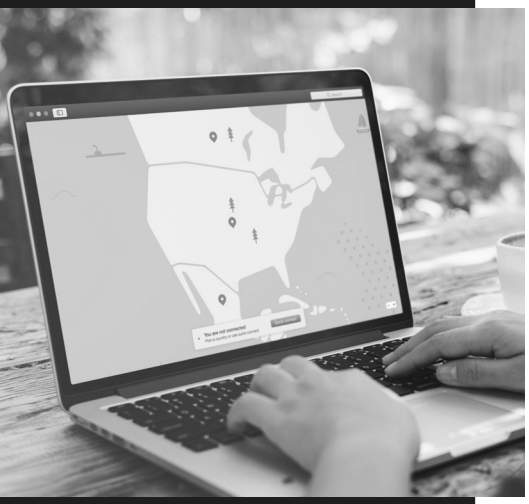
1. **Governance and Accountability:**
   A. Board approval of the cybersecurity policy and risk appetite.
   B. Assign CISO or equivalent accountable officer.
2. **Risk Management Framework:** Integrate cyber and IT risk into enterprise risk processes.
3. **Third-Party Risk Management:** Evaluate and monitor vendor security.
4. **Access and Identity Management:** Implement multi-factor authentication and least-privilege controls.
5. **Incident Management:**
   A. Maintain an Incident Response Plan.
   B. Report material cyber incidents to PA/FSCA promptly.
6. **Monitoring and Testing:**
   A. Conduct regular vulnerability assessments and penetration tests.
   B. Implement SOC monitoring or equivalent.
7. **Data Protection Alignment:** Ensure cyber controls align with POPIA safeguards.
8. **Focus Areas for 2026:**
   A. Incident reporting timelines.
   B. Cloud governance and outsourced IT monitoring.
   C. Integration of cybersecurity metrics into OMNI returns.

6. POPIA and Data Protection

Objective: To protect personal information and ensure lawful processing of client and employee data.

Key Requirements:

1. **Appoint and Register an Information Officer** with the Information Regulator.
2. **Maintain a Personal Information Inventory** and data flow map.
3. **Develop POPIA Policies and Privacy Notices.**
4. **Implement Security Safeguards:** Encryption, access controls, secure destruction of records.
5. **Obtain Consent and Limit Processing** to defined purposes.
6. **Ensure Operator (Third-Party) Compliance:** Contracts must include confidentiality and breach notification clauses.
7. **Respond to Data Subject Requests:** Enable access, correction, and deletion.
8. **Report Data Breaches:** Notify the Information Regulator and affected parties under Section 22.
9. **Conduct Periodic Privacy Impact Assessments (PIAs).**



Focus Areas for 2026: Integration of POPIA controls with cybersecurity governance and digital onboarding platforms.

7. Governance, Oversight, & Training

Board Responsibility:
  - Approve compliance frameworks and RMCP.
  - Review conduct, AML, cyber, and POPIA reports quarterly.
- **Compliance Function:** Coordinate regulatory reporting, monitor adherence, and maintain registers.
- **Risk and Internal Audit:** Test design and effectiveness of controls.
- **Training:**
  - AML / FICA awareness (FIC Section 43).
  - Conduct and Treat Customers Fairly (TCF).
  - Cybersecurity awareness and incident response.
  - POPIA and data handling practices.

All training must be documented and refreshed annually

8. Recordkeeping Summary

Record Type	Retention Period	Regulatory Reference
AML client and transaction records	5 years	FICA s22–24
Complaints register and conduct logs	5 years	FSCA TCF / COFI
OMNI Return and supporting evidence	5 years	FSCA reporting guidelines
Cyber incident logs and risk assessments	5 years	PA/FSCA Joint Standard
POPIA consents, notices, and breach reports	5 years	POPIA s14, 22

9. Compliance Checklist

Area	Key Requirement	Status
AML	RMCP implemented and reviewed	☐
Conduct	TCF and complaint management active	☐
Cybersecurity	Incident response plan tested	☐
POPIA	Information Officer registered	☐
OMNI Return	Submitted and documented	☐
Training	Annual compliance training completed	☐
Governance	Board minutes reflect compliance oversight	☐
Audit Trail	Documentation available for regulators	☐

Key Takeaways

- Financial institutions face integrated compliance expectations — governance, conduct, financial crime, cyber resilience, and data privacy are interconnected.
- The **OMNI Return** consolidates supervisory reporting — ensuring evidence-based compliance is critical.
- Proactive monitoring, training, and documentation demonstrate a mature compliance culture.
- Embedding compliance in business operations reduces regulatory, reputational, and operational risk.

About Navigate:

Founded in 2016, Navigate Compliance is a multidisciplinary governance, risk and compliance practice specialising in regulatory transformation, project management, and digital compliance innovation. We are experienced compliance professionals who manage and deliver high-impact compliance projects across regulated environments. Our services span end-to-end project delivery, specialised compliance resourcing, and hands-on execution—ensuring regulatory initiatives move from strategy to implementation with structure, control, and measurable outcomes.

Disclaimer

This handbook is provided for general information and educational purposes only. It is not intended to constitute legal, regulatory, financial, or professional advice, nor should it be relied upon as a substitute for detailed consultation or expert guidance. While every effort has been made to ensure the accuracy and relevance of the information contained herein, regulatory frameworks, industry standards, and best practices may evolve over time. Navigate does not accept any responsibility or liability for any loss, damages, or consequences arising from the use of this handbook or from decisions made based on its content. Users are encouraged to seek independent professional or legal advice before acting on any information provided in this document.

This publication does not create a client relationship between the reader and Navigate.

Navigate is a licensed compliance practice regulated by the Financial Sector Conduct Authority (FSCA), offering advisory, project management, regulatory resourcing, and governance solutions across the financial and regulated sectors. Navigate is also an accredited QCTO training provider, delivering professional qualifications, occupational programmes, and skills development pathways aligned to compliance, risk, IT governance, cybersecurity, digital ethics, and emerging technologies. In addition, Navigate provides specialist project management and resourcing services, including compliance leads, analysts, project managers, system integrators, and solution architects.

NAVIGATE COMPLIANCE

COMPLIANCE RE-IMAGINED

Let's Build Your Compliance Ecosystem

Book a consultation today

+27 73 956 9407

Johannesburg,
South Africa

info@navcompliance.co.za
www.navigatecompliance.io

Navigate is a licensed compliance practice regulated by the Financial Sector Conduct Authority (FSCA), offering advisory, project management, regulatory resourcing, and governance solutions across the financial and regulated sectors. Navigate is also an accredited QCTO training provider, delivering professional qualifications, occupational programmes, and skills development pathways aligned to compliance, risk, IT governance, cybersecurity, digital ethics, and emerging technologies. In addition, Navigate provides specialist project management and resourcing services, including compliance leads, analysts, project managers, system integrators, and solution architects.