Compliance Management Framework

Compliance Framework | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Compliance Management Framework
Document type	Compliance Framework
Jurisdiction	Global
Owner	Chief Compliance Officer
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose
2. Scope
3. Definitions
4. Regulatory Framework
5. Framework Architecture and Principles
6. Three Lines of Defence
7. Compliance Function Mandate and Independence
8. Obligations Identification and Regulatory Change Management
9. Compliance Risk Assessment Methodology
10. Controls Design and the Monitoring and Testing Program
11. Compliance Incident and Breach Management
12. Training and Awareness
13. Compliance Reporting
14. Compliance Culture
15. Roles, Responsibilities and Accountability
16. Framework Assurance and Annual Attestation
17. Breaches of this Framework
18. Review of this Framework
Appendix A: Obligations Register Template
Appendix B: Regulator Notification Obligations — Mapping Template
Policy Administration

1. Purpose

This Compliance Management Framework (the Framework) describes how the Company identifies, assesses, manages, monitors and reports on its compliance risk. It defines the architecture that connects the Company's Compliance Obligations to the people accountable for them, the controls that address them, the monitoring and testing that provides assurance over those controls, and the reporting that keeps management, the Board and regulators properly informed.

The Framework gives effect to the Company's obligation to maintain adequate compliance arrangements under applicable law in each of its operating jurisdiction(s), and is designed to satisfy the requirements of ISO 37301:2021 and the principles set out by the Basel Committee on Banking Supervision in Compliance and the compliance function in banks. It is a component of, and must operate consistently with, the Company's Risk Management Framework and Risk Appetite Statement. The Company has [no appetite / very low appetite] for deliberate or systemic non-compliance with its Compliance Obligations.

This Framework is approved by the Board of Directors and owned by the Chief Compliance Officer (CCO). It is a framework document rather than a policy: it describes components, how they interact and who is accountable for each, and it authorises the CCO to issue subordinate policies, procedures and standards that give it operational effect.

2. Scope

This Framework applies to the Company and all of its controlled entities, branches and representative offices, and to all directors, officers, employees, contractors and secondees (collectively, staff) in all jurisdictions in which the Company operates. It applies to all products, services, channels and business activities, including activities performed by service providers on the Company's behalf, for which the Company remains fully responsible.

The Framework covers all Compliance Obligations as defined in this document, including prudential, licensing, conduct, disclosure, financial crime, privacy, employment and consumer protection obligations. Specialist obligations that have their own dedicated frameworks or programs — including the AML/CFT Program, the Privacy Policy, the Whistleblower Protection Policy and the Risk Management Framework — remain subject to this Framework's obligations identification, register, incident management and reporting disciplines, and those documents must not be inconsistent with this Framework.

This Framework does not itself create Compliance Obligations; it establishes the system by which obligations arising elsewhere are identified and managed. Financial risk types (credit, market, liquidity and capital risk) are managed under their dedicated frameworks, although breaches of the prudential requirements governing those risks are Compliance Incidents for the purposes of section 11.

2.1 Jurisdictional application

This document states international best practice anchored to the standards listed in the Regulatory Framework section. The Company must map the requirements of this Framework to the law of each jurisdiction in which it operates, record the resulting jurisdiction-specific obligations in the Obligations Register, and complete the bracketed placeholders with the values required by applicable local law. Where the law of an operating jurisdiction imposes a stricter or additional requirement, local law prevails over this document.

3. Definitions

Term	Definition
Accountable Executive	A director or member of senior management to whom the Board or Chief Executive Officer has assigned named, documented individual accountability for a business line, function or material risk class of the Company, including any person registered, certified or designated under the senior manager accountability regime applicable in the Company's jurisdiction(s).
Attestation	A formal written confirmation by an accountable individual or staff member that, to the best of their knowledge after due enquiry, stated obligations, controls or requirements have been met for their area of responsibility during the relevant period, or that a document has been read and understood or remains current, together with disclosure of any known exceptions.
Breach	A failure, whether by act or omission, to comply with a mandatory requirement applicable to the Company, including a compliance obligation, a requirement of an approved policy where no exception has been approved in advance, or a Board-approved risk tolerance or limit, regardless of intent, materiality or subsequent justification.
Compliance Incident	Any event, act or omission that constitutes, or may constitute, a Breach, including near misses and control failures that did not result in an obligation being breached but revealed a weakness capable of doing so.
Compliance Obligation	A requirement with which the Company must, or has committed to, comply,

	arising from legislation, regulations, prudential and supervisory standards, licence and registration conditions, regulator directions, court and tribunal orders, industry codes to which the Company subscribes, and material undertakings given to regulators.
Compliance Risk	The risk of legal or regulatory sanction, material financial loss, restriction or loss of licence or authorisation, or damage to reputation that the Company may suffer as a result of a failure to comply with its Compliance Obligations. This definition is consistent with that used by the Basel Committee on Banking Supervision.
Compliance Function	The dedicated second-line function, led by the Chief Compliance Officer, responsible for the design, maintenance and oversight of this Framework and for independent advice, monitoring, testing and reporting on compliance risk.
Control	A policy, process, procedure, system, configuration, device, organisational arrangement or other practice designed and operated to maintain or modify risk, including preventive measures that stop a risk event or an instance of non-compliance from occurring and detective and corrective measures that identify it and reduce its impact.
Framework	This Compliance Management Framework, comprising the architecture, components, roles, processes and artefacts described in this document, together with the subordinate policies, procedures and registers that give it effect.
Governing Body	The Board of Directors of the Company, or, in a subsidiary or branch, the local board, management committee or equivalent body charged with governance of that entity, acting within the authority delegated to it.
Monitoring and Testing Program	The annual, risk-based program of compliance monitoring activities and independent testing of controls conducted or directed by the Compliance Function.
Obligation Owner	The business unit manager assigned in the Obligations Register as responsible for day-to-day compliance with a specific Compliance Obligation, reporting to the Accountable Executive for that business

	area.
Obligations Register	The Company's central register of compliance obligations, maintained under the Compliance Management Framework, recording for each obligation its source, jurisdiction, owner, risk rating, associated controls, monitoring activities and review status across the Company's operating jurisdictions.
Regulatory Change	Any new, amended or repealed legislation, regulation, supervisory standard, regulatory guidance, licence condition or industry code, in any jurisdiction in which the Company operates, whether in force, enacted, or at exposure-draft or consultation stage, that affects or may affect the Company's Compliance Obligations.
Reportable Breach	A Breach, suspected Breach or other event that applicable law in an operating jurisdiction requires the Company to notify to a regulator, supervisor, financial intelligence unit or other authority, within the timeframe and in the form prescribed by that law.
Three Lines of Defence	The Company's risk governance model allocating accountability across three lines: business and support units that own and manage risk and its controls (first line); the risk and compliance functions that set frameworks and provide independent oversight and challenge (second line); and Internal Audit, which provides independent assurance over both (third line).

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
ISO 37301:2021 Compliance management systems — Requirements with guidance for use	The international standard against which this Framework is designed; its requirements for leadership commitment, independence, compliance obligations identification, risk assessment, controls, performance evaluation and continual improvement structure this document.

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com