Risk Culture Framework

Risk 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	Risk Culture Framework
Document type	Risk Framework
Jurisdiction	Global
Owner	Chief Risk 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. Policy Statement and Principles
6. Sound Risk Culture: Definition and Elements
7. Behavioural Expectations
8. Governance and Oversight of Risk Culture
9. Risk Culture Assessment Methodology
10. Remuneration, Incentives and Consequence Management
11. Remediation of Risk Culture Weaknesses
12. Roles and Responsibilities
13. Reporting and Escalation
14. Breaches, Training and Review
Appendix A: Risk Culture Indicator Library
Appendix B: Risk Culture Survey — Core Question Set
Policy Administration

1. Purpose

This Framework defines what a sound risk culture means for the Company, sets the behavioural expectations that give effect to that culture, and establishes the methodology by which risk culture is assessed, monitored, reported and — where weaknesses are found — remediated. It exists so that the Board can discharge its responsibility, articulated in the BCBS Corporate Governance Principles for Banks and the G20/OECD Principles of Corporate Governance, to establish the Company's culture and values, to form a view of the Company's actual risk culture, to assess whether that culture supports the Company's ability to operate consistently within its risk appetite, to identify any desirable changes, and to ensure the Company takes steps to make those changes.

Risk culture determines whether the Company's formal risk architecture actually works. Policies, limits and controls only protect the Company when people identify risks honestly, escalate bad news early, challenge decisions constructively and accept accountability for outcomes. This Framework therefore concentrates on behaviour: what the Company expects of its people, how it measures whether those expectations are being met, and what happens when they are not. Its design draws directly on the four foundational indicators of a sound risk culture identified in the FSB Guidance on Supervisory Interaction with Financial Institutions on Risk Culture — tone from the top, accountability, effective challenge and incentives — and on the governance and culture component of the COSO Enterprise Risk Management framework.

This Framework is one component of the Company's risk document suite. The architecture of risk management is set out in the Risk Management Framework; the strategy for managing material risks and the three lines model are set out in the Risk Management Strategy; and the Board's appetite for risk is set out in the Risk Appetite Statement. This Framework does not restate those documents — it governs the cultural conditions needed for them to operate as intended, and should be read alongside them.

This Framework is approved by the Board of Directors and is owned and maintained by the Chief Risk Officer.

2. Scope

This Framework applies to the Company and all of its controlled entities, and to every person who performs work for the Company: directors, executives, permanent and fixed-term employees, contractors, secondees and agency staff. Behavioural expectations apply to all of these people; assessment, remuneration and consequence provisions apply to the extent each person participates in the relevant Company processes.

The Framework applies across all business lines, functions, products, channels and locations, including staff working remotely. It also extends, so far as the Company can reasonably influence them, to the personnel of material service providers acting on the Company's behalf: contractual arrangements and service provider governance under the Outsourcing Policy must require conduct consistent with the Behavioural Expectations section of this Framework when providers deal with the Company's customers or data.

Exclusions and boundaries: this Framework does not define the Company's risk appetite, risk classes, risk limits or risk management processes — these are governed by the Risk Appetite Statement, the Risk Management Framework and the Risk Management Strategy respectively. Detailed remuneration design is governed by the Remuneration Policy and Framework; detailed disciplinary procedure is governed by the Human Resources Policy and the Consequence Management Policy; whistleblowing protections are governed by the Whistleblower Protection Policy. Where those documents and this Framework intersect, this Framework sets the cultural requirements they must support.

Jurisdictional application: this Framework states international best practice, anchored to the FSB, BCBS, G20/OECD, COSO and ISO instruments cited in the Regulatory Framework section. The Company must map the requirements of this Framework to the law and regulatory expectations of each jurisdiction in which it operates — including any senior accountability regime, remuneration regulation, whistleblower protection law and employee data protection law — and where local law or a local regulator imposes a stricter or additional requirement, that local requirement prevails over this Framework.

3. Definitions

Term	Definition
Risk culture	The norms of behaviour, attitudes and shared assumptions of individuals and groups within the Company that shape the collective ability to identify, understand, openly discuss, escalate and act on current and future risks. Risk culture is the influence of organisational culture on how risk is taken and managed, consistent with the framing used by the Financial Stability Board.
Organisational culture	The shared values, beliefs and standards of behaviour that characterise the Company as a whole, embedded in its purpose, strategy and the way it treats its people, customers, regulators and community. Risk culture is a subset of organisational culture.
Sound risk culture	A state in which staff at all levels consistently make appropriate risk-based decisions, particularly under ambiguity, pressure or stress, and in which raising, discussing and acting on risk is normal, expected and safe.
Behavioural expectations	The specific, observable behaviours this

	Framework requires of directors, executives, people managers and staff in relation to risk-taking, escalation, challenge and accountability.
Tone from the top	The visible, consistent demonstration by the Board, CEO and Executive Team of the values and risk behaviours the Company expects of all staff, through their own decisions, communications and responses to adverse events.
Psychological safety	A working environment in which staff can raise concerns, admit errors, challenge decisions and report bad news without fear of blame, ridicule or retaliation.
Effective Challenge	Critical and constructive questioning of assumptions, decisions and proposals, before and during their implementation, by objective and informed parties with the standing, information and independence to identify limitations and require changes to the outcome; one of the foundational indicators of a sound risk culture identified by the FSB.
Risk culture indicator	A quantitative or qualitative measure used to assess an aspect of risk culture. Lead indicators signal emerging cultural conditions; lag indicators measure the outcomes culture has already produced.
Risk culture assessment	The structured annual process defined in this Framework by which the Company measures its actual risk culture against the Board's desired risk culture, using surveys, behavioural indicators and qualitative methods in combination.
Risk culture dashboard	The quarterly report of risk culture indicators, survey trends, consequence-management outcomes and remediation status provided to executive management and the Board Risk Committee.
Culture remediation plan	A documented, time-bound plan with a named executive owner to correct an identified risk culture weakness, including root cause, actions, milestones and effectiveness measures.
Consequence Management	The consistent and proportionate application of performance, remuneration, disciplinary and accountability outcomes where conduct, compliance or risk failures fall below the Company's standards, and of recognition where behaviour

	exemplifies them, consistent with the FSB Principles for Sound Compensation Practices.
Senior accountability regime	Any senior manager or executive accountability regime applicable in the Company's operating jurisdiction(s) under which named senior individuals hold documented responsibilities and owe duties of reasonable steps, and to which responsibility for risk culture must be mapped where such a regime applies.
Malus	An adjustment that reduces, including to zero, all or part of unvested or deferred variable remuneration before it vests, applied in response to misconduct, risk, conduct or culture outcomes or poor customer outcomes, consistent with the FSB Principles for Sound Compensation Practices and their Implementation Standards.
Clawback	The recovery from a person of some or all variable remuneration that has already vested in or been paid to that person, exercised in the circumstances permitted by applicable law, the person's contract, the terms of the relevant remuneration plan and the Company's remuneration arrangements.
Speak-up channels	The routes through which staff may raise risk or conduct concerns: line management, the Risk function, the People function, and the confidential whistleblowing channel operated consistently with ISO 37002 and any whistleblower protection law applicable in the Company's operating jurisdiction(s).
Three Lines Model	The Company's accountability model, based on the Institute of Internal Auditors' Three Lines Model, in which business and support units own and manage risk (first line), the risk and compliance functions set frameworks and provide oversight and challenge (second line), and Internal Audit provides independent assurance (third line).

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.