Operational Risk Policy

Risk Policy | 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	Operational Risk Policy
Document type	Risk Policy
Jurisdiction	Global
Owner	Chief Risk Officer
Approved by	Board Risk Committee
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Policy establishes the Company's requirements for identifying, assessing, managing, monitoring and reporting operational risk. It gives effect to the Basel Committee on Banking Supervision's Principles for the Sound Management of Operational Risk and Principles for Operational Resilience, which together require the Company to manage its operational risks effectively, maintain its critical operations within impact tolerances through severe disruption, and manage the operational risk arising from third parties.

The objective of this Policy is to ensure that the Company maintains a sound operational risk profile and remains operationally resilient: that losses, customer detriment, regulatory breaches and service disruptions arising from failed processes, people, systems or external events are prevented where practicable, detected quickly where not, and remediated in a way that prevents recurrence. Effective operational risk management protects depositors and other customers, the Company's financial soundness, and the Company's role in the markets and financial systems in which it operates.

This Policy forms part of the Company's Board-approved risk management framework and must be read with the Risk Appetite Statement. It has been approved by the Board Risk Committee under delegated authority from the Board. Accountability for the management of operational risk rests with the Chief Executive Officer and, within their respective areas, with the accountable first-line executives, including under any senior manager accountability regime applicable in the Company's jurisdiction(s). The Chief Risk Officer owns this Policy and is accountable for the design, adequacy and independent challenge of the operational risk framework, and not for the operational risks themselves.

2. Scope

This Policy applies to the Company and all of its subsidiaries and controlled entities, and to all directors, employees, contractors and secondees (together, staff). It applies to all business lines, products, channels, processes, systems, projects and change activity, and to operations performed on the Company's behalf by third parties, including through subcontractors and other parties in the supply chain.

This Policy covers all sources of operational risk, including process execution failure, internal and external fraud, technology and cyber risk, data risk, legal risk, people and employment practice risk, physical security and safety risk, model risk, change and project risk, and third-party and supply chain risk. Financial risks (credit, market and liquidity risk) are governed by their own policies; however, operational failures within credit, market or liquidity processes (for example, collateral processing errors or settlement failures) are operational risk events within the scope of this Policy.

This Policy operates alongside, and must be read with: the Risk Management Framework and Risk Appetite Statement; the Business Continuity Management

Policy and Business Continuity Plan; the Third-Party Risk Management Policy (which governs service provider arrangements in detail); the Issues and Incident Management Policy; the Information Technology Security Policy; and the Fraud Risk Management Policy. Where detailed requirements exist in those documents, this Policy sets the operational risk requirements they must satisfy and does not duplicate them.

Jurisdictional application. This Policy states international best practice, anchored to the standards listed in the Regulatory Framework section. The Company must map the requirements of this Policy to the laws and regulatory requirements of each jurisdiction in which it operates, including prudential rules on operational risk and resilience, incident notification obligations and outsourcing rules. Where applicable local law or a local regulator imposes a stricter or additional requirement, that requirement prevails over this Policy.

3. Definitions

Term	Definition
Operational risk	The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It includes legal risk, conduct-related operational failures, technology risk and the operational risk arising from third parties, but excludes strategic risk (although operational risk events may have strategic and reputational consequences).
Operational Resilience	The Company's ability to deliver critical operations through disruption, within Board-approved impact tolerances, by anticipating, preventing, withstanding, responding to, adapting to, and recovering and learning from operational risk events, consistent with the Basel Committee's Principles for Operational Resilience.
Critical Operation	An activity, process or service performed by the Company, or by a service provider on its behalf, which, if disrupted beyond the Company's impact tolerance, would cause material harm to depositors, customers or counterparties, pose a risk to the Company's safety and soundness, or impair its role in the financial system, consistent with the BCBS Principles for Operational Resilience.
Impact Tolerance	The Board-approved maximum level of disruption to a critical operation that the Company is willing to accept, assuming severe but plausible scenarios, expressed

	at a minimum as the maximum period of disruption, the maximum extent of data loss, and the minimum service level to be maintained while operating during disruption.
Operational Risk Event	A discrete occurrence arising from inadequate or failed internal processes, people or systems, or from external events, that has resulted or could have resulted in a financial loss, gain or near miss, or in a non-financial impact such as customer detriment, regulatory breach, data loss or service disruption.
Operational Risk Incident	An operational risk event that requires an active response, escalation or remediation, including an event arising at a service provider or other third party that has caused, or could have caused, loss or disruption to the Company or its customers.
Near Miss	An event that occurred and could have resulted in a loss or other adverse impact but did not, whether through controls operating as intended, timely intervention, corrective action or chance; near misses are recorded and analysed in the same manner as incidents.
Risk and Control Self-Assessment (RCSA)	The structured process by which business units identify their material risks, assess inherent risk, evaluate the design and operating effectiveness of key controls, determine residual risk against appetite and agree remediation actions.
Key Risk Indicator (KRI)	A quantified, forward-looking metric with defined thresholds or tolerance levels used to monitor changes in the level or trend of a risk exposure or in control effectiveness, and to trigger escalation and management action where risk appetite may be approached or breached.
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.
Issue	An identified weakness or gap in the design or operation of a control, a process

	deficiency, a policy breach, or a gap between the Company's risk profile and its risk appetite, arising from any source and recorded in the issues register for remediation through a tracked action plan.
Material third party	A service provider or other third party on which the Company relies to deliver a critical operation, or that exposes the Company to material operational risk, as determined under the Third-Party Risk Management Policy.
Scenario analysis	A forward-looking technique that assesses the impact of severe but plausible operational risk scenarios on the Company's risk profile, critical operations, financial position and impact tolerances.
Internal loss data	The Company's comprehensive record of operational risk losses and recoveries, maintained to the data quality standards required for operational risk management and, where applicable, for capital measurement under the Basel III standardised approach.
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).
Business Continuity Plan (BCP)	The Company's documented plan setting out how it would maintain critical operations within tolerance for disruption through a disruptive event and return to normal operations, including activation triggers, response and recovery actions, required resources and communications, prepared and exercised consistent with ISO 22301.

4. Regulatory Framework

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

Instrument / Standard	Relevance

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