Outsourcing Policy

Operational 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	Outsourcing Policy
Document type	Operational Risk Policy
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

The Company relies on service providers, including members of its own group, cloud providers and other third parties, to deliver services that support its operations, including operations that are critical to its customers and to its role in the financial system. While the Company may transfer the performance of an activity to a service provider, it cannot transfer its accountability for that activity or for the risks the arrangement creates. This principle of retained accountability is common to every major international framework governing third-party risk.

This Policy sets out the Company's requirements for identifying, assessing, contracting, monitoring and exiting service provider arrangements. It is anchored to the Financial Stability Board's toolkit for third-party risk management and oversight (2023), the Basel Committee's Principles for Operational Resilience and Principles for the Sound Management of Operational Risk, and, as a reference model, the European Banking Authority's Guidelines on Outsourcing Arrangements. Consistent with these frameworks, this Policy applies a risk-based lens to all service provider arrangements, not only to activities that were previously performed in-house.

This Policy forms part of the Company's operational risk management framework. It operates alongside, and must be read with, the Operational Risk Policy (which governs critical operations, tolerance levels and incident management), the Business Continuity Plan and Business Continuity Management Policy (which govern response to disruption), and the Procurement Policy (which governs the sourcing and purchasing process). This Policy is approved by the Board of Directors and owned by the Chief Risk Officer.

2. Scope

This Policy applies to the Company and all of its controlled entities, and to all directors, employees, contractors and secondees involved in proposing, approving, managing or monitoring service provider arrangements.

This Policy applies to all arrangements under which a service provider performs a service for the Company, including:

- arrangements with members of the Company's group and intra-group service arrangements, which must be managed with the same rigour as arm's-length arrangements;
- cloud arrangements, software-as-a-service and other technology-delivered services;
- cross-border arrangements, wherever the provider is incorporated;
- arrangements entered into before the effective date of this Policy, which must be brought into compliance at the earlier of their next renewal or [24] months from that date, or any earlier date required by the Company's regulator.

The Chief Risk Officer must maintain a remediation plan for those arrangements, recording for each the gaps, a named remediation owner and the compliance date. Where an arrangement will not comply by the date required, the

relationship owner must escalate to the Chief Risk Officer within [5] business days, and the Chief Risk Officer must either approve a time-limited extension, recorded in the policy exceptions register maintained under the Material Service Providers and the Register section, or require exit under the Exit Strategies and Termination section. Any extension beyond [6] months, or affecting a critical operation, requires Board Risk Committee approval, and the Board Risk Committee must set a final compliance date and direct exit where it is not met.

This Policy does not apply to one-off purchases of goods, utilities supplied on standard public terms, membership of industry bodies, market infrastructure participation governed by scheme rules, or employment arrangements. Where it is unclear whether an arrangement is in scope, the Chief Risk Officer determines the question, applying the principle that substance prevails over the label given to the arrangement.

Boundary with the Procurement Policy: the Procurement Policy governs how the Company identifies needs, runs tenders, selects suppliers and executes purchases. This Policy governs the risk assessment of service provider arrangements before entry and the ongoing management of service provider risk for the life of the arrangement. Both apply to the establishment of a new arrangement; the requirements of this Policy cannot be satisfied by compliance with the Procurement Policy alone.

Jurisdictional application: this Policy states international best practice for the management of service provider arrangements. The Company must map the requirements of this Policy to the laws and regulatory requirements of each jurisdiction in which it operates, including local rules on outsourcing approval, notification, registers, data transfer and regulator access. Where the law of a jurisdiction imposes a stricter or additional requirement, local law prevails over this Policy.

3. Definitions

Term	Definition
Service provider	Any party, including a member of the Company's own group, that provides a service to the Company under an arrangement, whether or not the service was previously performed in-house and whether the arrangement is described as outsourcing, managed services, cloud services or otherwise.
Third-party arrangement	Any arrangement under which a service provider performs a service for the Company, including intra-group arrangements, cloud arrangements and arrangements delivered from another jurisdiction.
Material Service Provider	A third party, including an intra-group provider, on which the Company relies to

	deliver a critical operation or to manage a material risk, or whose failure or compromise would otherwise expose the Company to material operational, financial, technology or compliance risk, together with material subcontractors in its supply chain, as recorded in the Company's service provider register.
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.
Tolerance level	The Board-approved maximum level of disruption to a critical operation the Company is willing to accept, expressed as a maximum period of disruption, maximum extent of data loss and minimum service level during disruption. Equivalent to the impact tolerances described in international operational resilience frameworks.
Material arrangement	An arrangement with a material service provider for the provision of a service falling within the basis on which that provider was assessed as material.
Fourth party	A party engaged by a service provider (a sub-contractor or other downstream provider) on which the service provider relies, in whole or in part, to deliver a service to the Company; the extended chain of such parties is the Company's third-party supply chain.
Sub-contracting	The engagement by a service provider of another party to perform all or part of a service that the service provider has contracted to deliver to the Company.
Cross-border arrangement	An arrangement under which a service provided to the Company, or the data supporting it, is performed, processed or stored in a jurisdiction other than the jurisdiction(s) in which the Company operates, regardless of where the service provider is incorporated.
Cloud arrangement	A service provider arrangement under which computing resources (including

	infrastructure, platforms or software) are delivered on a shared, on-demand basis, typically involving data hosted outside the Company's own environment.
Concentration Risk	The risk that the Company's aggregate exposure to, or dependence upon, a single counterparty, group of connected counterparties, industry sector, geographic region, funding source, asset class or service provider is large enough that failure of that single point could cause disproportionate loss or threaten earnings, capital or viability.
Exit strategy	A documented, executable approach for ceasing a material arrangement, including transfer to an alternative provider, bringing the service in-house or discontinuing the service, in both orderly and stressed circumstances.
Stressed exit	An exit from a material arrangement executed under adverse conditions, such as sudden provider failure, insolvency, contract termination for cause, or a regulatory or geopolitical event, where normal transition timeframes are not available.
Third-party register	The Company's register of all material service providers and material arrangements maintained under the Material Service Providers and the Register section of this Policy and made available to the Company's prudential regulator where required by applicable local law.
Due diligence	The structured assessment of a prospective or existing service provider's financial and non-financial capacity, controls and risk profile performed before entry into, and periodically during, an arrangement.
Relationship owner	The accountable executive or senior manager assigned ownership of a service provider arrangement, responsible for its day-to-day management, performance monitoring and escalation.
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

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