Business Continuity Management 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	Business Continuity Management Policy
Document type	Operational 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 framework by which the Company maintains the ability to deliver its critical operations through severe but plausible disruptions. It sets out how the Company identifies its critical operations, establishes Board-approved tolerance levels for disruption, develops and maintains credible continuity and recovery arrangements, tests those arrangements, and responds to and reports disruptions when they occur.

The Policy is designed to meet the Basel Committee on Banking Supervision's Principles for Operational Resilience and its Principles for the Sound Management of Operational Risk, and is structured to satisfy the requirements of ISO 22301 for a business continuity management system. It operates as a component of the Company's operational risk management framework and must remain consistent with the Company's recovery and resolution planning for severe financial stress and with any tolerance for disruption set or directed by the Company's prudential regulator.

In any disruption, the safety and welfare of the Company's staff, customers and visitors takes priority over the resumption of business activity. Subject to that priority, the Company's objective is to maintain each critical operation within its tolerance levels and to return to normal operations promptly once a disruption has ended.

This Policy is approved by the Board Risk Committee on the recommendation of the Chief Risk Officer, who owns the Policy and is responsible for its maintenance and annual review.

2. Scope

This Policy applies to the Company and all of its controlled entities, and to all directors, employees, contractors and contingent workers. It applies to all business units, products, channels, premises, systems and data, whether operated by the Company or by a service provider on its behalf, in every jurisdiction in which the Company operates.

The Policy covers disruptions of any cause, including loss of premises, loss or failure of technology or data, cyber attack, loss or unavailability of people (including pandemic), failure of a service provider, and failure of utilities or market infrastructure. It applies regardless of whether the disruption originates within the Company, at a material service provider, or in the wider environment.

Detailed response documentation — the Business Continuity Plan, Crisis Management Plan, Disaster Recovery Plan and business-unit recovery procedures — sits beneath this Policy and must comply with it. Financial resilience in severe stress is addressed by the Company's recovery and resolution planning and is outside the scope of this Policy, although continuity arrangements must remain consistent with those plans.

Jurisdictional application: this Policy states international best practice, anchored to ISO 22301 and the Basel Committee's Principles for Operational Resilience. The Company must map the requirements of this Policy to the law and regulatory requirements of each jurisdiction in which it operates, including any local rules on operational resilience, impact tolerances, outsourcing and incident notification. Where local law or a local regulator imposes a stricter or additional requirement, that requirement prevails over this Policy.

3. Definitions

Term	Definition
Business Continuity Management (BCM)	The Company-wide discipline of identifying threats of disruption to critical operations and building the capability to maintain or restore those operations within Board-approved tolerance levels.
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.
Business Impact Analysis (BIA)	The structured assessment of the Company's business processes to determine their criticality and interdependencies, the impacts that would arise over time from their disruption, and the recovery time objectives, minimum acceptable service levels, resources and dependencies required for recovery, undertaken consistent with ISO 22301 and ISO/TS 22317.
Critical Operations	The processes and services undertaken by the Company or by its service providers which, if disrupted beyond the Company's defined impact tolerances, would have a material adverse impact on depositors, other customers or counterparties, on the Company's safety and soundness, or on its role in the financial system.
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.
Tolerance Levels	The Board-approved limits for each critical operation comprising the maximum period of disruption the Company would tolerate, the maximum extent of data loss it would accept, and the minimum service levels it would maintain while operating under alternative arrangements.
Maximum Period of Disruption	The Board-approved maximum time a critical operation may be unavailable or degraded below its minimum service level before the impact on customers or the financial system becomes intolerable.
Recovery Time Objective (RTO)	The target period, set shorter than the applicable maximum tolerable period of disruption, within which a business process, system or critical operation must be restored to at least its defined minimum service level following a disruption.
Recovery Point Objective (RPO)	The maximum tolerable amount of data loss for a process or system, expressed as a period of time measured backwards from the point of disruption, being the point in time to which data must be recoverable following a disruption.
Minimum Service Level	The reduced but acceptable level of output, throughput or service quality for a critical operation or business process that the Company commits to maintain, or to resume operating at, during a period of disruption while working under alternative arrangements.
Disruption	Any event, whether anticipated or unanticipated, that interrupts or degrades the normal operation of the Company's processes, systems, premises, people or service providers.
Severe but Plausible Scenario	A disruption scenario that is extreme yet credible for the Company's business model, operating environment and dependencies, used to set impact tolerances and to test whether critical operations can be maintained within them; a scenario need not have previously occurred to be plausible.
Crisis Management Team (CMT)	The standing senior executive team, chaired by the Chief Executive Officer or delegate and constituted under the Company's crisis management

	arrangements, with overall authority to direct the Company's response to a declared incident, crisis or severe disruption, including activation of business continuity, recovery and related plans.
Disaster Recovery Plan (DRP)	The technology component of the Company's continuity arrangements, documenting the procedures, resources and priorities for recovering the information technology infrastructure, applications and data that support critical operations, and operating under the direction of the Business Continuity Plan.
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.
Alternate Site	A pre-arranged premises or working arrangement, including remote working, from which critical operations can be temporarily resumed or performed when a primary site or capability is unavailable.
Tolerance Breach	A disruption in which a critical operation is not maintained within one or more of its Board-approved tolerance levels.

4. Regulatory Framework

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

Instrument / Standard	Relevance
ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements	The international standard against which the Company's BCM programme is designed, including the BIA, continuity strategies, plan documentation, exercising and continual improvement required by this Policy.
ISO 22313:2020 Business continuity management systems — Guidance on the use of ISO 22301	Implementation guidance applied in operationalising the requirements of this Policy, including the design of continuity strategies and the exercise programme.
ISO/TS 22317:2021 Guidelines for	Informs the Company's BIA methodology,

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