Business Continuity Plan

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

Contents

1. Purpose

This Business Continuity Plan sets out how the Company responds to an incident that disrupts, or threatens to disrupt, its people, premises, technology, data or service providers. It exists so that, when a disruption occurs, the Company can protect life and safety, maintain its critical operations within the Board-approved tolerance for disruption, meet its obligations to depositors, customers, counterparties and regulators, and return to normal operations in an orderly way.

This Plan is the operational component of the Company's business continuity management system, designed to align with ISO 22301 and the BCBS Principles for Operational Resilience. The Business Continuity Management Policy establishes governance, the business impact analysis and tolerances for disruption; this Plan converts those into action: who may activate the response, how incidents are classified, who commands the response, what recovery strategies apply to each loss scenario, in what sequence critical operations are recovered, and how the Company communicates throughout.

This Plan is approved by the Chief Executive Officer under authority delegated by the Board and is owned by the Chief Risk Officer, who is accountable for keeping it current, tested and capable of activation at any time. Accountability for business continuity and technology recovery must be clearly allocated to named executives under the senior manager accountability regime applicable in the Company's jurisdiction(s).

2. Scope

This Plan applies to the Company and all of its business units, sites and channels, to all directors, employees, contractors and secondees, and to all critical operations identified in the business impact analysis and recorded in Appendix B, whether performed by the Company or by a material service provider on its behalf. It applies to any disruption scenario, including but not limited to loss of a site, loss of technology or data, loss or unavailability of people, failure of a material service provider, and cyber events.

This Plan directs, and is supported by, the following subordinate documents: the Disaster Recovery Plan (technology recovery procedures, owned by the Chief Information Officer); the Information Security Incident Response Plan and its playbooks; the Crisis Communications Plan (detailed messaging, scripts and spokesperson protocols); the emergency evacuation procedures for each site; and service-provider contingency plans. Where an incident engages one of those documents, its procedures are executed under the command structure established by this Plan.

This Plan does not address financial stress or capital and liquidity recovery, which are governed by the Company's Recovery and Exit Plan and Contingency Funding Plan, nor business-as-usual incident management for events below the activation criteria in Section 5. Where a single event engages both this Plan and the

Recovery and Exit Plan, the Chief Executive Officer must ensure a single command structure with clearly assigned leadership for each workstream.

Jurisdictional application: this Plan states international best practice, drawing on ISO 22301 and the BCBS operational resilience framework. The Company must map the requirements of this Plan to the law and regulatory expectations of each jurisdiction in which it operates — in particular incident and outage notification obligations, data breach regimes, and health and safety duties — and where local law or the Company's regulator imposes a stricter or additional requirement, that requirement prevails.

3. Definitions

Term	Definition
Activation	The formal decision, made by an authorised person under the governance arrangements of the relevant plan, to invoke that plan, mobilising the designated response or crisis management team and moving the Company to the applicable response, recovery or exit footing.
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.
Battle box	A secured physical and electronic collection of the documents, credentials, equipment and records needed to execute this Plan when normal systems and premises are unavailable, as listed in Appendix D.
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 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.
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.
Event log	The chronological record of decisions, actions, notifications and information received during an incident, maintained in the format at Appendix E.
Incident	An event that has occurred or is imminent, arising from inadequate or failed processes, people, systems or external events, that disrupts or is reasonably likely to disrupt the Company's people, premises, technology, data, service providers or critical operations, or to cause customer, financial, regulatory, conduct or reputational impact.
Incident classification level	The severity rating (Level 1 to Level 3) assigned to an incident under Section 6, which determines the response structure, authority and communication cadence.
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.
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.
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.
Stand-Down	The formal decision, taken against the stand-down criteria in the relevant plan, that crisis or incident response arrangements are no longer required, by which the response is de-escalated or closed and management of any residual activity reverts to business-as-usual structures.
Tolerance for Disruption	The Board-approved maximum level of disruption to a critical operation that the Company is prepared to accept under severe but plausible scenarios, expressed as a maximum period of disruption, a maximum extent of data loss and a minimum service level to be maintained, consistent with the impact-tolerance concept in the BCBS Principles for Operational Resilience.
Work area recovery	Alternative working positions, equipment and connectivity allowing staff to perform critical operations away from their normal workplace.

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	The international standard for business continuity management; this Plan

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