Business Continuity Test Program

Operational Risk Program | 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 Test Program
Document type	Operational Risk Program
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 Test Program (the Program) sets out how the Company plans, conducts, evaluates and reports the testing of its business continuity arrangements. ISO 22301 requires an organisation to exercise and test its business continuity strategies and solutions through a planned programme that validates them over time, and the BCBS Principles for Operational Resilience expect a bank to demonstrate its ability to deliver critical operations through disruption, within Board-approved tolerances, under severe but plausible scenarios — including disruptions originating with material service providers. This document is the mechanism by which those requirements are met.

The Program exists to provide the Board, senior management and the Company's prudential regulator with credible, evidence-based assurance that the Business Continuity Plan (BCP), Crisis Management Plan and supporting recovery arrangements are current, workable and effective — not merely documented. It converts continuity planning from a paper exercise into a tested capability by specifying the types of test the Company uses, the minimum frequency of testing by criticality, how scenarios are designed, how success is judged against tolerances for disruption, and how findings are remediated and reported.

This Program is owned by the Chief Risk Officer, approved by the Chief Executive Officer, and noted by the Board Risk Committee (BRC) as part of its oversight of operational resilience. It operates alongside, and gives effect to, the Business Continuity Management Policy; where this Program and that Policy conflict, the Policy prevails.

2. Scope

This Program applies to the Company and all of its controlled entities, and to all directors, employees, contractors and secondees who hold a role in the Company's continuity, crisis management or recovery arrangements, whether as decision-makers, responders, participants or observers.

The Program covers testing of:

- the BCP and all business unit recovery plans supporting critical operations;
- the Crisis Management Plan, including crisis communications arrangements;
- IT disaster recovery arrangements for systems supporting critical operations;
- workplace recovery arrangements, including alternate sites and remote working at scale;
- continuity arrangements of material service providers, including joint testing; and
- operational readiness to support the applicable deposit insurance scheme or resolution authority, where the Company is required to maintain such capability.

Routine preventative maintenance (such as data backup verification), security penetration testing, and testing of the Company's recovery and resolution plans are governed by their own programmes and are outside the scope of this document, although their results are considered when scheduling tests under this Program. Real disruptions in which continuity arrangements are activated are not tests, but must be subject to a post-incident review commissioned, led and completed in accordance with the Business Continuity Plan, which establishes who may lead such a review, the timeframes for commissioning and completing it, and the independence requirements that apply where a person held a crisis role during the incident. That review must additionally satisfy the evaluation, findings and reporting requirements of the Success Criteria and Results Evaluation, Findings, Remediation and Tracking, and Reporting and Escalation sections of this Program, and an activation may be credited against the annual schedule only in accordance with the Credit for Real Activations requirements below.

Jurisdictional application: this Program states international best practice, anchored to ISO 22301 and the Basel Committee's operational resilience and operational risk principles. The Company must map the requirements of this Program to the law and regulatory expectations of each jurisdiction in which it operates — including any locally prescribed testing frequencies, notification obligations and evidence requirements — and where local law or a local regulator imposes a stricter requirement, that stricter requirement prevails.

3. Definitions

Term	Definition
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.
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 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.
Exercise Programme	The planned, systematic programme of exercises and tests required by ISO 22301 clause 8.5, of which this document is the Company's implementation.
Desktop / Walkthrough Test	A facilitated, discussion-based exercise in which participants step through their documented continuity responsibilities against a hypothetical scenario without activating systems or relocating operations.
Scenario Simulation	A time-pressured exercise in which the crisis management structure responds in real time to an evolving scripted scenario, including injects, decision points and communications, without full operational recovery.
Functional Component Test	An operational test that activates a discrete component of continuity arrangements, such as recovery of a single system, activation of an alternate work site, or execution of the call-out tree.
Full Failover Test	An operational test in which production processing for a system or critical operation is transferred to, and run from, its designated recovery environment or site.
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.
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.
Test Sponsor	The accountable executive who owns a scheduled test, approves its scope, objectives and scenario, and is

	accountable for remediating findings that arise from it.
Test Facilitator	The person appointed to design, run and control a test, including preparing the scenario, briefing participants, managing injects and compiling the test report.
Observer	A person appointed to independently record events, decisions, timings and issues during a test without participating in the response.
Finding	A documented control weakness, non-compliance, error, breach or improvement opportunity identified through an audit, assurance or testing activity, rated for severity and recorded in the relevant findings register with an accountable owner and an agreed remediation due date.
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.
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.
Board Risk Committee (BRC)	The committee of the Board with delegated oversight of the Company's risk management framework, including operational resilience and business continuity.

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.