Business Impact Analysis

Operational Risk Analysis | 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 Impact Analysis
Document type	Operational Risk Analysis
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 document sets out the Company's methodology and template for conducting Business Impact Analysis (BIA). The BIA is the analytical foundation of the Company's operational resilience arrangements: it identifies the Company's business processes, assesses the impact of their disruption over time, and determines the recovery objectives, minimum service levels and resource dependencies that drive business continuity planning, disaster recovery design and investment decisions.

International standards and supervisory expectations — in particular ISO 22301, ISO/TS 22317 and the Basel Committee's Principles for Operational Resilience — require the Company to identify its critical operations, set Board-approved impact tolerances for each, map the internal and third-party dependencies on which they rely, and maintain a credible Business Continuity Plan (BCP) capable of keeping critical operations within tolerance through severe but plausible disruption. The BIA is the mechanism by which the Company generates the evidence for each of these obligations. BIA outputs feed directly into the identification and classification of critical operations, the proposal of impact tolerances for Board approval, the register of material service providers, and the scenario selection for BCP exercising.

This document has been approved by the Chief Executive Officer on the recommendation of the Chief Risk Officer, who owns the methodology. It is designed to produce consistent, comparable and defensible results across all business units, so that the Company's continuity investment is directed to the processes where disruption would cause the greatest harm to customers, the Company and the financial system.

2. Scope

This methodology applies to all business units, divisions and legal entities of the Company in every jurisdiction in which it operates, including support and enabling functions such as technology, finance, treasury, human resources, risk, compliance and legal. It applies to processes performed in-house and to processes performed in whole or in part by service providers, including intra-group providers and material service providers.

All business processes within scope must be captured in the process inventory described in section 6. Every process in the inventory must receive at least a triage-level assessment; processes assessed as potentially critical or high-impact must receive a full BIA using the questionnaire at Appendix A.

This document governs the analysis of disruption impacts and the setting of recovery requirements. It does not itself set out response and recovery procedures, which are contained in the Business Continuity Plan, the Disaster Recovery Plan and associated incident response documents. Nothing in this document displaces obligations under the Company's Operational Risk Management Framework or Board-approved Risk Appetite Statement.

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

3. Definitions

Term	Definition
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.
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.
Maximum Tolerable Period of Disruption (MTPD)	The maximum period for which a business process can be unavailable before the resulting impacts become unacceptable to the Company, its customers or its regulators. The MTPD is an impact-driven ceiling, not a recovery target.
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.
Process Owner	The manager accountable for the day-to-day performance of a business process, and for the accuracy and currency of the BIA information recorded for that process.
Dependency	A resource without which a business process cannot operate at its minimum service level, including people, technology systems, data, premises, equipment and third-party services.
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.
Single Point of Failure	A dependency for which no substitute, workaround or redundant capacity exists, such that its loss alone would prevent a business process from meeting its minimum service level.
Peak Period	A recurring or foreseeable period during which the volume, value or time-criticality of a business process is materially elevated, such that the impact of a disruption would be greater than at other times.
Workaround	A documented manual or alternative procedure that allows a business process to continue at or above its minimum service level while a primary dependency

	is unavailable.
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.
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.
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.
BIA Results Register	The consolidated record of all completed BIA assessments, maintained in the form set out at Appendix B, which constitutes the authoritative source of recovery objectives and dependency information for continuity planning.

4. Regulatory Framework

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

Instrument / Standard	Relevance
BCBS Principles for Operational Resilience (Basel Committee on Banking Supervision, 2021)	Establishes supervisory expectations that banks identify critical operations, set tolerances for disruption and map internal and third-party dependencies; the BIA is the principal analytical mechanism by which the Company meets these expectations.
BCBS Revised Principles for the Sound Management of Operational Risk (2021)	Requires business continuity planning grounded in an analysis of the criticality of operations and their interdependencies,

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.