IT Change Control Policy

IT 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	IT Change Control Policy
Document type	IT Policy
Jurisdiction	Global
Owner	Chief Information 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 Policy establishes the mandatory controls governing changes to the Company's production technology environment. Its purpose is to ensure that every change is properly assessed, authorised, tested, scheduled, implemented and verified, so that the benefits of change are delivered without unacceptable disruption to services, critical operations or customers.

Poorly managed change is a leading cause of operational incidents in financial institutions. The Basel Committee's Principles for Operational Resilience and Principles for the Sound Management of Operational Risk expect the Company to manage the risks arising from change so that its critical operations remain within defined impact tolerances, and ISO/IEC 27001 requires formal change management to preserve the security of information and systems. This Policy operationalises those expectations by requiring proportionate, risk-based control over all changes, from routine pre-approved activities through to major transformations and emergency fixes.

This Policy has been approved by the Chief Executive Officer. It is owned and maintained by the Chief Information Officer, who is accountable for its implementation and for the effectiveness of the change management process it mandates.

2. Scope

This Policy applies to the Company and all of its controlled entities, and to all directors, employees, contractors, consultants and third-party personnel who initiate, approve, implement or verify changes to the Company's production technology environment.

In-scope changes include, without limitation, changes to: applications and application code; infrastructure, operating systems and middleware; databases and data structures; networks, firewalls and security controls; cloud services and cloud configurations; batch schedules and interfaces; end-user computing solutions that support critical operations; and technology changes initiated by third-party service providers that affect the Company's services.

The following are excluded from this Policy: changes confined entirely to isolated development or test environments with no production data and no production connectivity; content updates made through approved business-as-usual publishing tools with their own approval workflow; and data corrections executed under the Company's separate [data management procedure], provided they are logged and auditable. Exclusions do not remove the obligation to protect production data and services.

Jurisdictional application: this Policy states international best practice. The Company must map its requirements to the law and regulatory expectations of each jurisdiction in which it operates, including any local rules governing outsourcing, operational resilience, incident notification and data protection.

Where local law or a local regulator imposes a stricter requirement than this Policy, the stricter local requirement prevails.

3. Definitions

Term	Definition
Change	Any addition, modification, decommissioning or removal of technology infrastructure, applications, system configurations, data structures, network components, security controls or supporting documentation that could affect production IT services.
Standard Change	A low-risk, repeatable change with a pre-approved, documented procedure and a known, tested outcome, which may be implemented without individual Change Advisory Board approval.
Normal Change	A change that is not a Standard or Emergency Change and that must follow the full assessment, approval, testing and scheduling requirements of this Policy. Normal Changes are classified as minor or major based on the change risk rating.
Emergency Change	A change that must be implemented urgently to restore service, prevent imminent service failure, or remediate a security vulnerability under active or imminent exploitation, and for which the normal approval lead time cannot be met.
Change Advisory Board (CAB)	The forum that reviews, challenges and approves changes in accordance with this Policy, and oversees the forward schedule of change.
Emergency CAB (eCAB)	The minimum quorum of authorised approvers convened at short notice to authorise an Emergency Change.
Change Record	The auditable record of a change in the change management system, containing the mandatory contents described in this Policy from initiation to closure.
Backout Plan	A documented, tested set of steps to restore a system or service to its pre-change state (or an equivalent safe state) if a change fails or produces unacceptable impact. Also referred to as a rollback plan.
Change Window	A pre-agreed period during which approved changes may be implemented, selected to minimise impact on critical

	operations and customers.
Freeze Period	A defined period during which no changes other than approved Emergency Changes may be implemented, such as financial period-end processing or designated peak business periods.
Failed Change	A change that is backed out, causes an incident, does not achieve its intended outcome, or requires unplanned remedial work within [5] business days of implementation.
Unauthorised Change	Any change to a production environment implemented without an approved Change Record, or materially outside the scope, method or schedule that was approved.
Break-glass Access	Emergency privileged access to production systems granted outside normal access provisioning, used only where standard access paths are unavailable or too slow to prevent material harm.
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.
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.
Post-Implementation Verification	The structured checks performed after a change is deployed to confirm the change achieved its intended outcome and that affected services, interfaces and controls operate correctly.
Change Initiator	The person who raises a Change Record and is accountable for the completeness and accuracy of its contents.
Change Implementer	The person or team that executes the approved implementation steps within the approved change window.
Configuration Item	Any component of the technology

	environment recorded in the configuration management database (CMDB) whose state is subject to change control.
Forward Schedule of Change	The consolidated calendar of approved and proposed changes, change windows and freeze periods maintained by the change management function.

4. Regulatory Framework

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

Instrument / Standard	Relevance
ISO/IEC 27001:2022 — Information Security Management Systems	Annex A control 8.32 (Change management) requires changes to information processing facilities and systems to be subject to formal change management procedures that preserve information security.
ISO/IEC 27002:2022 — Information Security Controls	Provides implementation guidance for change management controls, including planning, testing, approval, rollback and communication requirements applied throughout this Policy.
BCBS Principles for Operational Resilience (2021)	Expects banks to manage change so that critical operations remain within impact tolerances, and to assess the resilience implications of changes to technology, processes and third-party arrangements.
BCBS Revised Principles for the Sound Management of Operational Risk (2021)	Identifies inadequately managed change as a leading source of operational risk and requires change risk to be assessed, approved and monitored within the operational risk management framework.
ITIL 4 — Change Enablement Practice	The service management good-practice model for change classification (standard, normal, emergency), change authority assignment, CAB operation and the forward schedule of change adopted by this Policy.
ISO/IEC 20000-1:2018 — IT Service Management	Requires a defined change management process covering assessment, approval, scheduling, review and unsuccessful-change handling for services within the service management system.
NIST Cybersecurity Framework 2.0	Configuration and change management controls (PR.PS) support the protect function; detection of unauthorised

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