Issues and Incident 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	Issues and Incident 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 sets out the Company's enterprise-wide requirements for identifying, recording, classifying, escalating, remediating and reporting issues and incidents. It exists so that problems are found early, fixed at their root cause, escalated to the right level of authority at the right time, notified to regulators within mandated timeframes, and used to strengthen the control environment rather than recur.

The Policy implements the incident management expectations of the BCBS Principles for Operational Resilience and the BCBS Principles for the Sound Management of Operational Risk, and connects them with the Company's obligations under applicable information security, data protection, conduct, anti-money laundering and accountability regimes in each jurisdiction in which it operates. It applies to all categories of issue and incident — operational, technology, compliance, conduct, data, fraud, third-party and people-related — not only information technology events.

This Policy is approved by the Board Risk Committee and owned by the Chief Risk Officer. It forms part of the Company's operational risk management framework and must be read alongside the Risk Management Strategy, Operational Risk Management Framework, Business Continuity Plan, Whistleblower Protection Policy and Breach Reporting Procedure.

2. Scope

This Policy applies to the Company and all of its controlled entities, and to all directors, employees, contractors, secondees and agency staff. It applies across all products, services, channels, business units and support functions, and to issues and incidents arising from or involving material service providers and other third parties engaged by the Company.

In scope are all issues (control weaknesses and gaps identified before harm has occurred), all incidents (events that have occurred, whether or not a loss crystallised), and all near misses. This includes operational disruptions, information security and cyber events, personal data breaches, compliance and regulatory breaches, conduct events, fraud (internal and external), third-party and outsourcing failures, model failures, and events affecting critical operations.

The following are governed by companion documents but must be cross-referenced to this Policy where they arise from, or give rise to, an incident or issue: customer complaints (Dispute Resolution Policy), whistleblower disclosures (Whistleblower Protection Policy), workplace health and safety incidents (Health and Safety Policy), business continuity invocation (Business Continuity Plan) and formal regulatory breach reporting decisions (Breach Reporting Procedure). Board and committee action items are tracked separately and are not issues for the purposes of this Policy.

Jurisdictional application: this Policy states international best practice drawn from the frameworks cited in the Regulatory Framework section. The Company must

map the requirements of this Policy to the laws and regulatory requirements of each jurisdiction in which it operates, including local incident notification triggers and deadlines, and where local law imposes a stricter or additional requirement, local law prevails.

3. Definitions

Term	Definition
Issue	An identified weakness or gap in the design or operation of a control, a process deficiency, a policy breach, or a gap between the Company's risk profile and its risk appetite, arising from any source and recorded in the issues register for remediation through a tracked action plan.
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.
Near Miss	An event that occurred and could have resulted in a loss or other adverse impact but did not, whether through controls operating as intended, timely intervention, corrective action or chance; near misses are recorded and analysed in the same manner as incidents.
Material Incident	An operational risk incident that materially affects, or has the potential to materially affect, the Company's operations, its ability to deliver critical operations within tolerance for disruption, or its depositors and customers, triggering notification to [the Company's prudential regulator] within the timeframe prescribed by applicable local law.
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.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data held by the Company or by a processor on its behalf, which may require notification to the relevant data protection authority and to affected individuals under applicable local law.
Reportable Regulatory Breach	A breach, or likely breach, of a licence condition or legal or regulatory obligation that meets the reporting threshold set by applicable law, requiring notification to [the Company's conduct regulator or other competent authority] within the prescribed timeframe.
Root Cause Analysis (RCA)	A structured investigation to identify the underlying cause(s) of an incident or issue — not merely its symptoms — so that remediation prevents recurrence.
Read-Across	A structured assessment of whether the root cause of an incident or issue also exists in similar products, processes, systems, entities or third-party arrangements, so that systemic exposures are remediated once, everywhere.
Incident Manager	The accountable individual assigned to coordinate the response to an incident, including containment, assessment, notification, remediation and closure.
Issue Owner	The accountable individual (at [manager level or above]) responsible for an issue and delivery of its action plan through to evidence-based closure.
Action Plan	A documented set of specific, measurable, time-bound actions, each with a named owner and due date, designed to remediate the root cause of an issue or incident.
Risk Acceptance	A formal, time-bound decision by a holder

	of appropriate delegated authority to accept the residual risk of an issue rather than remediate it, recorded in the issues register with rationale and review date.
Consequence Management	The consistent and proportionate application of performance, remuneration, disciplinary and accountability outcomes where conduct, compliance or risk failures fall below the Company's standards, and of recognition where behaviour exemplifies them, consistent with the FSB Principles for Sound Compensation Practices.
GRC System	The Company's governance, risk and compliance system of record ([system name]) in which all issues, incidents, near misses, action plans and closure evidence must be recorded.
Financial Intelligence Unit (FIU)	The national agency in each jurisdiction in which the Company operates that acts as the central authority for receiving, analysing and disseminating suspicious transaction reports and other information relevant to money laundering, associated predicate offences, terrorism financing and proliferation financing, consistent with the FATF Recommendations.
Lines of Defence	The Company's accountability model: Line 1 (business and support units that own and manage risk), Line 2 (risk and compliance functions that oversee and challenge) and Line 3 (internal audit, providing independent assurance).

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 (2021)	Requires incident management programmes that identify, respond to, recover and learn from incidents affecting critical operations, tested against Board-approved tolerances for disruption.
BCBS Revised Principles for the Sound Management of Operational Risk (2021)	Requires the identification, reporting, escalation and root cause analysis of operational risk events, comprehensive internal loss data, and use of event data

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