



INTEGRUM

Regulatory Update

06 March 2026

www.integrum-sg.com

CONSULTATION ON UPDATED GUIDELINES ON OPERATIONAL RISK MANAGEMENT

06 March 2026

INTRODUCTION

The Monetary Authority of Singapore (“**MAS**”) has proposed updated Guidelines on Operational Risk Management (the “**proposed ORMG**”) that would supersede the existing Guidelines on Risk Management Practices – Operational Risk, which were published in March 2013 and applicable to all financial institutions (“**FIs**”) in Singapore.

The proposed ORMG reflects the growing importance of operational risk management in an era of increasing digitalisation, heavier reliance on third-party service providers, and a heightened threat of cyber-attacks. These are built on MAS' existing expectations and incorporate key elements of guidance by the Basel Committee on Banking Supervision (“**BCBS**”), specifically the Revised Principles for the Sound Management of Operational Risk.

This regulatory update identifies the key proposals under consultation and evaluates the potential operational impact it could have on the FIs, pre and post implementation.

This publication is provided by Integrium for educational and informational purposes only and is not intended and should not be construed as providing legal or other advice.

EXPANDED GUIDANCE ON ORM FRAMEWORK

The proposed ORMG provides key proposals (discussed below) and expanded guidance on building an effective operational risk management framework which includes timely identification, assessment, management, monitoring, and reporting of operational risks. The MAS also highlights the need for strong governance, clear risk appetite/tolerance definitions, consistent terminology, documented policies and procedures, monitoring thresholds, and independent reviews.

The proposed ORMG also introduces a detailed three-lines-of-defence model where business units manage risks day-to-day, the independent ORM function designs and challenges the framework, and internal audit provides independent assessment and reporting to the board.

The proposal highlights that board ultimately remains responsible for operational risk oversight, setting the risk culture, and establishing senior management-level ORM committee with diverse expertise, as applicable, while senior management implements and manages the framework, ensures adequate resourcing, and keeps the board informed of key operational risk developments. Additionally, it also highlights the use of tools such as risk and control assessments, key risk indicators, loss data analysis, scenario analysis, and benchmarking to monitor and manage operational risks effectively.

We discuss below the key new proposals in this consultation paper.

KEY PROPOSALS

Risk-Proportionate Implementation

MAS proposes applying the proposed ORMG to all FIs, as defined in Section 2 of the Financial Services and Markets Act 2022 (“FSMA”). However, FIs may implement the expectations in a proportionate manner (commensurate with their size and complexity), taking into account the nature and the materiality of risks in their business operations.

In practical terms, this means that a small broker-dealer licensed with MAS, for example, would not be expected to maintain the same level of operational risk infrastructure as a large domestic bank. However, for smaller FIs, even with proportionate implementation, this may represent a meaningful uplift in operational risk management capabilities.

Public Disclosure Requirements

One of the most significant new proposal is the requirement for Domestic Systemically Important Banks or Insurers (“D-SIBs/D-SIIs”) to publicly disclose their approach to operational risk management and their operational risk exposures. MAS also proposes that these institutions make their code of conduct publicly available, so stakeholders can assess how effectively risks are identified, monitored, and mitigated. They should also disclose significant operational loss events, while avoiding creating additional risk (e.g., exposing control weaknesses). A board-approved disclosure policy with regular independent review would be required.

For the code of conduct, D-SIBs/D-SIIs without a website must provide it upon request, and foreign FIs may adopt a group code subject to review for suitability in Singapore.

Operationally, this could mean additional board training, more frequent ORM reporting cycles, the creation of new governance committees or subcommittees, and careful consideration of what information to disclose without inadvertently creating additional

operational risk, such as alerting bad actors to unaddressed control vulnerabilities, etc, as applicable.

Change Management

MAS proposes that FIs implement a robust change management process to identify, assess, and manage operational risks arising from planned changes. This includes clear policies, approval procedures, and adequate resourcing to monitor risks over time.

The proposed ORMG highlights that changes in risk profiles may stem from new products, activities, markets, processes, or IT systems. Reviews should consider risk appetite, controls, and monitoring metrics, with ongoing monitoring during and after implementation to detect any material deviations from expected risk levels.

In practice, this could be particularly relevant for major transformation initiatives such as cloud migration, vendor transitions, mergers and acquisitions, cybersecurity enhancements and the rollout of AI-enabled tools. The changes could trigger an operational review including aspects of technology, business continuity, and outsourcing.

Oversight of Branches and Subsidiaries

MAS proposes that FIs should consider the operational risks of their branches and subsidiaries, including those overseas, when looking at risks across the whole group, especially if they are supervised on a consolidated basis or own critical information infrastructure. They should ensure these entities follow an operational risk framework aligned with the updated ORMG.

For FIs in Singapore with a head office overseas, they can use their global framework but must add local requirements where needed to meet MAS guidelines.

In terms of impact, this could reinforce the oversight from the head office and increased coordination with the Singapore compliance teams, alongside a need for additional manpower and operational considerations.

CONCLUSION & PRACTICAL OBSERVATIONS

The proposed ORMG represents a substantial evolution from the concise, high-level former guidelines to a comprehensive, detailed, and prescriptive framework. The most notable new elements are the public disclosure requirements for systemically important institutions, the dedicated change management section, the three-lines-of-defence model, the expanded ORM tool guidance, and the requirement for consolidated oversight of branches and subsidiaries.

For CEOs, the key message is that operational risk management is no longer a back-office compliance exercise but a board-level strategic priority. The explicit linkage between business strategy, risk appetite, and operational risk governance signals MAS' expectation that ORM should inform business decision-making at the highest levels.

For compliance officers, the practical impact is that gap analyses should begin promptly. While there will be a six-month transition period, for most firms with mature ORM frameworks that timeline could be tight. Firms will need to consider and build new capabilities, hire specialist staff, and implement new governance structures.

For the general public and stakeholders, the public disclosure requirements for D-SIBs / D-SIIs would enhance transparency and market discipline, enabling customers and investors to better understand how major financial institutions manage operational risk and conduct.

FIs may find it helpful to consider the following near-term steps during the consultation period.

- Bring together teams from Risk, Compliance, Legal, IT, Procurement, Operations, and other relevant business units to review the proposals in a coordinated manner.
- Compare existing frameworks with consultation proposals to identify areas where additional information, governance, or system visibility may be needed if the proposals are implemented.
- Gain a clearer understanding of AI tools, model-based vendors, and AI-related service dependencies across the organisation, so they can be assessed as part of overall third-party and operational risk.

Contacts

Mark Jacobsen

Founder
Integrum

E mark@integrum-sg.com

Dewansh Raheja

Senior Manager
Integrum

E dewansh.raheja@integrum-sg.com

Integrum Pte. Ltd.
Level 19
Singapore Land Tower
50 Raffles Place
Singapore 048623
www.integrum-sg.com