SAI360
RISK FROM EVERY ANGLE

Japan's Global Push Raises the Stakes for Integrated Risk Management

Table of Contents

Introduction

Japan's largest financial institutions are doubling down on global expansion. Nomura's ~$1.8 billion acquisition of Macquarie's US and European asset management businesses in 2025 marked a significant move as the firm renewed focus on international growth to rebalance its geographic revenue mix.[1]

Nomura is emblematic of a wider trend across Japan's major institutions. Mizuho and MUFG have both indicated intent to acquire or partner with overseas asset managers in Europe and the US. Leading insurers, Dai-ichi Life and Meiji Yasuda, also acquired or took strategic stakes in overseas firms to strengthen their global footprint last year.[2]

Collectively, these moves signal a decisive vote of confidence in global growth opportunities and in Japanese institutions' ability to compete and succeed in international markets.

Scaling across borders, however, demands a structural shift in how institutions design their operating models, govern cross-border activities, and manage risk. Success hinges on strategic execution, and risk management must play a central role in shaping the strategy from the outset.

1. https://www.ft.com/content/e5c4e302-abc3-4a05-9903-e70aa9681319
2. https://www.reuters.com/business/finance/mizuho-mufg-join-race-by-japans-banks-money-manager-deals-overseas-2025-08-25/

The Operating Environment: rising supervisory and operational pressure

International expansion materially raises the bar for risk management. As firms operate across jurisdictions, integrate acquisitions, and rely on more complex technology and third-party ecosystems, risks that were once contained become more interconnected and difficult to manage.

The nature of risk changes across multiple dimensions:

Risk Type	Considerations with international expansion
Operational Risk	Increased complexity from divergent operating models, legacy systems, data architectures, and expanded outsourcing arrangements across jurisdictions.
Compliance Risk	Heightened supervisory expectations in Europe, the UK, and the US, including stricter standards for governance, documentation, and control effectiveness.
Technology & Cyber Risk	Greater reliance on integrated platforms, third-party vendors, cloud infrastructure, and cross-border data flows.

Traditionally, firms attempt to manage this complexity with outdated systems and siloed data; these structural deficiencies have a real business impact:

- **Fragmented risk visibility:** Without alignment, risk teams may implement controls that compliance can't attest to, or compliance may report on effectiveness without grounding in operational reality.
- **Gaps in control assurance:** Each function operates with partial data, leading to blind spots in risk across the organization.
- **Duplication and inefficiency:** Overlapping processes, duplicated effort, and inconsistent workflows can waste resources and increase compliance costs.

Japanese Regulatory Signals: Expectations for Integrated Risk Management (IRM)

March 2025 Guidelines from the Japan Financial Services Agency (FSA) point to a more explicit, control-based supervisory expectations across a broad and interconnected set of risk typologies, with particular emphasis on:[3]

- demonstrable control effectiveness, not just policies
- continuous review of residual risk
- board-level visibility
- third-party and cloud dependencies as first-order risks, not peripheral ones

In other words, the FSA is focused on how risks are actually controlled, monitored, and tested. IT risk, cyber risk, and outsourcing risk are not treated as separate domains; they are explicitly connected. This is a de facto integrated risk view, even if the FSA doesn't use that terminology explicitly.

While these expectations are not yet hard-coded into primary regulations, they serve as the benchmark for supervisory inspections and directly inform business improvement orders and remediation programs.

Past supervisory actions show that regulators have limited tolerance for weaknesses in group risk governance, particularly where issues are systemic.

In November '21, Mizuho Financial Group was issued a business improvement order by the FSA following a series of eight system outages over ten months.

The recurring incidents pointed to deficiencies in:

- system risk management required to maintain stable system operations,
- governance regime and/or
- organizational culture.

Mizuho's response – a multi-year integrated risk reform program – illustrates the scale of change now expected by supervisors.

The cost of acting late is high, and going forward, institutions will not be afforded the same tolerance for post-incident reform.

Risk management and governance reforms are clear supervisory priorities in Japan, alongside tighter expectations for operational resilience, especially in network and technology risk.[4] As supervisory scrutiny intensifies, Japanese institutions face mounting pressure to strengthen their risk frameworks to promote sustainable domestic and international growth.

3. https://www.fsa.go.jp/common/law/guide/kinyushohin_eng.pdf
4. https://www.imf.org/-/media/files/publications/cr/2024/english/1jpnea2024004.pdf

Building an IRM Framework

In other jurisdictions, expectations around IRM are already formalized. Europe, in particular, has established a clear regulatory direction that, while not always labeled as "integrated risk management", effectively mandates it in practice.

The Digital Operational Resilience Act (DORA)[5] and the Critical Entities Resilience Directive (CER) move beyond siloed risk disciplines, requiring firms to assess operational, technology, cyber, and third-party risk within a single framework.[6]

The sections that follow examine what an IRM framework comprises, drawing on best practices from EU regulators and FSA commentary, where applicable.

What is an IRM framework?

An organization-wide approach to identifying, assessing, managing, and monitoring all material risks, individually and in aggregate. A defining feature of modern IRM is its "all-hazards" perspective – covering natural, physical, human-made, and cyber risks – a concept explicitly referenced in the CER Directive.

Who is Responsible for IRM?

Senior management must play an active role in overseeing the development, implementation, and continuous refinement of the IRM framework. While accountability has traditionally sat with the Chief Risk Officer, or equivalent, the breadth and interconnectedness of the modern risk landscape mean this responsibility cannot be confined to a narrow circle of risk managers. Legal, compliance, IT, HR, and business leaders all need a seat at the table

Japan's FSA places responsibility on the board for "development and establishment of the legal compliance and internal control environment". So, while ownership may be distributed across functions – and across the globe – in day-to-day operations, the board and senior leaders remain accountable for the effectiveness of that system across the entire organization, including international subsidiaries and overseas operations.

5. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR
6. This regulatory direction is not confined to Europe. Comparable expectations are evident in Australia, with APRA CPS 230, and in the UK via the FCA's Operational Resilience Act.

What Does an IRM Framework Look Like?

1. Build Visibility European regulators consistently expect organizations to protect "important" or "critical" business services – those whose disruption could cause intolerable harm to customers or pose systemic risk. The FSA classifies "critical functions" as those "where failure would lead to severe disruption of the financial system".

There is no single codified definition of "intolerable harm," so firms must use defensible thresholds based on their operating model, customer base, geographical footprint and associated regulatory context.

A top-down approach works best. Start by creating a centralized inventory of all products and services. This must be done at the subsidiary (national) and group level. Establishing this consolidated view enables consistent prioritization across the entire business.

Criticality must be assessed with a structured impact assessment (IA). IA's commonly leverage a mix of qualitative and quantitative metrics:

- **Customer impact:** number of customers affected, duration of outage, severity of detriment
- **Financial impact:** revenue loss, remediation costs, liquidity impact
- **Regulatory impact:** likelihood of breaches or size of penalties

Once critical services are identified, document the people, processes, technology, data, facilities, and third- and fourth-party dependencies that support each service. The goal is to expose interdependencies, identify single points of failure, and understand how disruption could cascade.

2. Assess Risk When categorizing critical or important services, impact is assessed through the lens of customer and market harm. This is a service-level, outcome-based assessment. The next step is to determine the impact at the risk-scenario level. Here, "impact" focuses on the extent to which a certain threat might degrade the service and how far a disruption would propagate across systems or processes.

An accompanying likelihood assessment should consider:

- The strength and maturity of existing controls.
- Historical incidents and near misses – the FSA explicitly asks firms to "take notice of illegal incidents or lapses at other companies".
- Exposure to external risk drivers such as geography, cyber threat levels, or market volatility.
- Internal capacity constraints, including skills, staffing, and operational complexity.

Integration is challenging given the breadth of risks involved. This complexity is further compounded by international expansion, where differing regulatory frameworks and locally embedded nomenclature can hinder consistency and alignment. To make this manageable, leaders must strive to standardize risk categories and definitions across the group – using established frameworks such as MITRE ATT&CK for cyber risk may prove useful.

Consistent terminology improves communication and supports aggregation. Centralizing risk information allows firms to see, in one place, which risk scenarios pose the greatest threat to each critical service and where mitigation efforts should be prioritized.

3. Mitigate Risk Risk cannot be eliminated. But regulators expect risk-aligned control environments supported by centralized visibility.

For effective mitigation, controls must operate across three reinforcing layers:

- Technical controls embedded in systems and infrastructure (e.g., multi-factor authentication or rules to encrypt or mask information)
- Operational controls executed through processes (e.g., incident response and failover mechanisms)
- Organizational controls embedded in governance, accountability, and culture (e.g., regular staff training).[7]

This is an established concept in cyber risk management, particularly under the Network and Information Security Directive 2 (NIS2), but the structure translates cleanly into integrated risk management beyond cybersecurity.

Centralized visibility enables firms to identify duplicative, misaligned, or excessive controls, as well as gaps. Rationalizing controls is often as important as adding new ones.

7. Both customers and regulators now expect downstream organizations to implement robust controls that can identify, prevent, and mitigate risk within the supply chain.

How IRM Promotes Resilience

European regulatory frameworks do not treat risk management and resilience as separate objectives – they explicitly link the two. Risk management focuses on preventing disruption, and resilience is the ability to maintain critical operations and recover rapidly when incidents inevitably occur. Regulators increasingly view these as inseparable, and supervisory expectations now reflect this symbiotic relationship.

A similar emphasis is clearly emerging in Japanese supervisory guidance. Language from the FSA mirrors the resilience-oriented framing seen in Europe, particularly around preparedness, continuity, and recovery. The FSA stresses the importance of maintaining essential operations during disruption, noting that financial institutions must be able to "take recovery measures quickly and ensure that the minimum necessary operations and services are maintained".

Integrated risk management turns resilience from a theory into an operational capability. Bringing services, dependencies, risks, and controls into a single framework gives firms a full, end-to-end view of how disruption might unfold.

- **Scenario testing:** Integrated risk data enables realistic scenario analysis by showing the full, end-to-end impact of disruptions across services, systems, processes, and third parties, including cumulative and cascading effects.
- **Incident response and reporting:** Clear visibility of dependencies allows faster, more coordinated incident response, supporting rapid impact assessment, root-cause identification and reporting.
- **Business continuity:** Integration aligns recovery actions with critical services, ownership, and recovery priorities to ensure the continuity of essential operations during disruptions.

The Business Imperative

The financial cost of disruption is significant. Operational disruptions can erode up to 3% of annual revenue, driven by halted services and remediation costs.[8] Data risk compounds this exposure: the average cost of a data breach in Japan reached approximately $3.65 million in 2025,[9] and over 21,000 personal information breaches were reported in fiscal year 2024, a 58% year-on-year increase.[10]

The market impact extends beyond direct losses. Operational disruptions erode investor confidence. McKinsey's analysis of 500 operational risk events (2006 2020) found equity losses five times greater than direct financial losses.[11]

International expansion raises the stakes. While an EU regulation, DORA applies to EU subsidiaries and authorized branches of non-EU institutions and carries potential fines of up to 2% of total annual worldwide turnover, alongside intrusive supervisory remediation.

But this isn't just a cost-saving story. Japanese institutions need to seize the moment. Integrated risk management enables firms to do exactly that. It allows firms to better adapt to regulatory change, secure cross-border licenses, maintain client confidence after incidents, and integrate acquisitions at speed and scale. In a crowded global market, IRM is emerging as an important competitive differentiator.

8. https://www.fastly.com/resources/industry-report/security/cybersecurity-at-the-crossroads-japan-2025
9. https://www.ibm.com/reports/data-breach
10. https://english.news.cn/20250610/1a728143a0ff4e79a03718c7772ab9c6/c.html
11. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/response-and-resilience-in-operational-risk-events

A Smart Approach to Transformation

An IRM framework should enable stakeholders across the organization to generate data-driven insights for the board and senior management, supporting more informed, risk-aware decision-making. Data sits at the heart of this shift. Building a scalable compliance and risk architecture capable of supporting growth requires technology and automation; without it, modern information flows become unmanageable.

Change management is a key consideration, particularly for institutions with a global footprint. Each firm is different, typically supported by a mix of legacy systems, manual processes, and point solutions. Growth through acquisition can also mean inheriting subpar or disjointed risk management frameworks. Success depends on creating consistency quickly, but in a way that is manageable and minimally disruptive.

Avoid Accumulating Controls

This shouldn't be a rip-and-replace exercise, nor is it about implementing more controls or deploying technology for its own sake. Excessive or poorly aligned controls introduce friction, create false assurance, and often increase operational risk rather than reduce it.

Technology should rationalize controls, not multiply them, and ensure that effort is focused where risk is highest.

A Phased Approach Is Essential

GRC modernization, therefore, must be approached as a journey rather than a single "big-bang" transformation event. Organizations should move deliberately from manual processes to digitized workflows, and ultimately to integrated risk and compliance management.

Attempting to bypass intermediate stages often results in fragmented implementations that fail to deliver value. A phased approach allows firms to stabilize processes, improve data quality, and build confidence before advancing toward deeper integration.

Foundation First

Digitize core processes before exploring deeper integration. Transition systematically from manual to automated to integrated. Replace spreadsheets, email-based reviews, and static documents with structured automated workflows. Digitizing core components — risk assessments, policy management, regulatory change tracking, and training – sets the stage for integration. The objective is efficiency, consistency, and auditability.

Integration is only achievable once these foundations are in place. IRM is most effective when enabled through a GRC platform that connects previously siloed activities and data. This allows firms to link risks to controls, policies, incidents, and regulatory obligations, and to trace issues and remediation actions back to underlying control weaknesses. Unifying risk and compliance activities on a single GRC platform also enables enterprise-wide visibility, predictive analytics, and more intelligent, forward-looking risk management.

Analytics allows CROs to replace intuition with objective, data-backed decisions, transforming risk management from reactive to proactive by uncovering insights that would otherwise remain hidden.

Integration is a Strategic Imperative for Japanese Institutions

Japan's largest financial institutions are entering a decisive phase of global expansion. Domestic and international supervisory signals are clear – firms need demonstrable control effectiveness. This demands continuous oversight and an integrated view of how risks interact across the entire business.

IRM is a prerequisite for sustainable growth. Integration enables boards and senior management to see risk as it truly exists across the enterprise, to understand how disruptions cascade, and to make informed decisions with confidence. It reduces duplication, strengthens resilience, accelerates post-merger integration, and supports regulatory credibility in overseas markets.

The choice is not whether to integrate, but how deliberately and how soon. Those that invest early in integrated risk, compliance, and governance architectures will be better positioned to scale internationally, absorb regulatory change, and compete on equal footing with global peers. Tolerance for failure is diminishing, and IRM offers a new way to obtain a strategic advantage.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform that spans the entire risk and compliance spectrum.

- Whistleblower and Case Management
- Ethics & Compliance Training
- Policy Management
- Conflicts of Interest
- Incident Management
- Regulatory Compliance
- Regulatory Obligations
- Horizon Scanning
- Enterprise & Operational Risk Management
- Third-Party Risk
- Internal Audit
- Internal Controls
- IT Risk
- Business Continuity
- Vendor Risk Management