FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

APRIL 2026

Operational resilience thematic: findings and insights – derivatives issuers

Introduction

In 2025 the Financial Markets Authority – Te Mana Tātai Hokohoko (FMA) surveyed derivatives issuers as part of our thematic review of operational resilience. We would like to thank all derivatives issuers that participated. Their openness and willingness to share insights has provided a valuable foundation for understanding sector maturity and identifying opportunities for collective growth.

The purpose of this survey was to understand the sector's overall level of operational resilience maturity and to support continuous improvement in a constructive and collaborative way. It is also designed to deepen our understanding of risks and potential harm associated with weaknesses in operational resilience and gain a better understanding of current practices.

By voluntarily sharing experiences and practices, those who participated demonstrated a genuine desire to strengthen operational resilience for the benefit of their organisation, their customers, and New Zealand's financial markets.

About the thematic

This survey was undertaken to support the FMA's regulatory priority of identifying emerging risks and opportunities, to support market integrity and transparency, and resilient markets and providers – as outlined in our 2025 Financial Conduct Report.

The survey asked about core resilience components such as governance, outsourcing, incident management, business continuity planning, technology systems resilience, information security, and mandatory notification practices. It was designed to gather insights into how firms embed operational resilience into their frameworks and day-to-day processes, identify strengths and gaps, and inform practical guidance for continuous improvement.

Participants were invited to complete the survey via an online form, which remained open for several weeks. Responses were voluntary and captured both qualitative and quantitative aspects of operational resilience practices.

The assessment applied a five-level maturity scale (Initial to Optimised) across the core operational resilience components identified in the survey. Each area was evaluated against a structured criteria and,

based on the participant's response, a score was attributed to each entity. The rating for each resilience component has been included in the sector takeaways section of the report.

It is important to note the survey relied on self-reported information, and the FMA has not independently verified the responses from participants.

Sector takeaways

With participation from more than half of the sector, derivatives issuers are demonstrating positive progress towards operational maturity. This document highlights the sector's strengths, acknowledges areas for further development, and provides practical and supportive recommendations. The FMA is committed to working alongside derivatives issuers, giving guidance and fostering a collaborative environment where good practice can be shared.

Governance

Financial resources: All respondents indicated they have sufficient financial resources to invest in operational resilience and technology systems, although the scale of investment varies significantly across the sector (responses include less than 1% and more than 10% of annual revenue of the surveyed entities).

Board capabilities: All respondents have at least one board member with operational resilience expertise. Only some respondents include training on operational resilience as a regular board agenda item. Most boards receive training 'as needed', which may limit their ability to stay ahead of emerging risks.

Risk management: Risk management frameworks for operational resilience are widely in place. Self-assessment scores range from 4 to 5 out of 5, indicating effective application across the sector.

Compliance culture: Most boards and senior management regularly discuss operational resilience. All respondents have remediation procedures for non-compliance. Scores are high (4 to 5 out of 5), reflecting strong confidence in the board's support for fostering a culture of compliance.

Awareness of obligations: All boards rate their awareness of operational resilience obligations highly (4 to 5 out of 5).

Overall governance scores for each entity ranged from 4.3 to 4.9 out of 5.

Outsourcing

Use of providers: Half of the respondents outsource their key functions and indicated it is relatively easy to switch providers due to availability of alternative providers in the market. Respondents who outsourced key business functions externally reported a significant reliance on external service providers for the delivery of these functions.

Overseas providers: All respondents that have outsource arrangements in place indicated that they rely on overseas-based service providers and reported awareness of the related risks and regulatory requirements.

Due diligence: While most respondents demonstrate robust due diligence arrangements across key risk areas, a small number have only basic written procedures.

Performance monitoring: The respondents that have outsource arrangements in place actively monitor their service providers, with formal agreements that include business continuity and technology requirements. However, some outsourced arrangements are reviewed only at renewal, which does not align with the risk-appropriate frequency requirement of the standard conditions for derivatives issuer licences (**DI standard conditions**).

Formal agreements: While the respondents that have outsource arrangements in place have formal agreements with their providers, the agreements do not include comprehensive provisions for performance monitoring, remedial actions for non-performance, and continuity.

Overall outsourcing scores for each entity ranged from 3.5 to 5.0 out of 5.

Incident management and business continuity plans (BCP)

Documented BCPs: All respondents have documented BCPs, but the inclusion of key components is inconsistent. Some respondents indicated that their BCP documents do not encompass outsource arrangements as required by the DI standard conditions.

Implementation: All respondents have internal controls to support the implementation of BCP procedures; however not all have verified the effectiveness of these controls. Most respondents have previously activated their BCP in response to a disruption and rated the effectiveness of the BCP high. The survey shows that BCP training is widely provided - primarily on an annual basis with most respondents training senior management and frontline staff, but only a few providing training to board members.

Testing and updates: Some respondents do not test BCPs regularly as required by the DI standard conditions. All respondents who conduct BCP testing confirmed that results are communicated to the board and/or senior management, with the majority reviewing and approving the results and a minority actively discussing them and providing direction on remediation actions. As far as updates are concerned, survey responses suggest that all respondents would update their BCP due to material changes of business location, structure, or operations.

Compliance knowledge: Most respondents indicated that it is easy to comply with business continuity and technology systems requirements, with self-assessment scores of 4 or 5 out of 5.

Overall incident management and BCP scores for each entity ranged from 3.6 to 4.9 out of 5.

Technology and information security

System complexity: Most respondents indicated that they have a significant reliance on critical technology systems that have been specifically tailored to their organisation's needs. Some respondents noted significant customisation of their critical technology systems. The majority reported that it would be moderate to very difficult to replace these systems. Some respondents reported use of legacy systems for core operations for about 5-20% of their core operations.

Staff capability: Respondents reported having an adequate number of competent staff to support critical technology systems. Most indicated that they have invested in staff training and are confident in the level of investment in training.

Investment in upgrades: Most respondents have recently upgraded their critical technology systems and cybersecurity, with no adverse impacts reported from underinvestment. However, a small portion of respondents did not specify when their last major upgrade occurred, limiting visibility over the adequacy of their technology investment.

Information security frameworks: Adoption of recognised frameworks (such as NIST and ISO/IEC 27001) is low, with only a small number of respondents reporting their use and most indicating limited familiarity with these frameworks.

Monitoring and detection: Most respondents have measures in place to monitor and detect activity that could impact the operational resilience of their critical technology systems. However, some respondents indicated that they do not have the capability to monitor for anomalous activities on an ongoing basis, or information is collected with a material time delay.

Customer data protection: All respondents are confident in their ability to protect customer data.

Overall technology and information security scores for each entity ranged from 3.7 to 4.5 out of 5.

Incident notification

Materiality criteria: All respondents use clear criteria (e.g. customer impact, cost, regulatory consequences) to determine incident materiality. The effectiveness of decision-making process for determining materiality were highly rated at 4 or 5 out of 5.

Identification procedures: All respondents have established procedures to identify incidents, but some respondents indicated that the effectiveness of these procedures have not been tested.

Knowledge of requirements: Self-assessment scores are generally high across the respondents.

Overall incident notification scores for each entity ranged from 4.2 to 5.0 out of 5.

Overall assessment

Sector maturity

Although we have not independently verified the responses, feedback from participants suggests that most derivatives issuers believe their operational resilience is at a relatively mature level. Findings suggest there is room to strengthen capability across the assessed areas. The sector has built a strong foundation in operational resilience, with frameworks and processes in place. This demonstrates an awareness of the importance of being resilient to disruptions and taking proactive steps to mitigate related risks. The survey results highlight several areas where the FMA believes further attention and improvement are needed, as outlined below:

Opportunities for improvement

Board and Staff Capability

Strengthening board and senior management engagement

Boards generally have access to operational resilience expertise; however, survey responses indicate that training on this topic is often informal and ad hoc. Implementing more regular and structured operational resilience training programmes would help boards and senior management maintain visibility of emerging risks and keep their knowledge of operational resilience current.

Compliance

Strengthening compliance oversight and frameworks for reporting

While survey responses indicate strong board support for a culture of compliance with operational resilience, the topic is not consistently discussed at board or senior management level. Strengthening compliance oversight through a structured framework for reporting, clearer accountability and regular discussions would support more consistent and demonstrable compliance outcomes.

Compliance

Strengthen assurance with internal controls

Compliance-related controls are not applied consistently across organisations. Although documented procedures are generally in place, their application varies across business areas, limiting assurance over compliance outcomes. More consistent embedding of procedures and structured control testing would strenghthen assurance and improve visibilty for boards and senior management.

Business continuity planning

Continuous improvement of business continuity arrangements

While all respondents have documented BCPs, their testing and review practices are inconsistent. More regular scenario-based testing, timely updates following material changes, and active board engagement with test outcomes would help ensure BCPs remain effective and operationally useful.

Business continuity planning

Ensuring comprehensive BCP coverage

BCPs should include provisions for outsourcing arrangements and cover key components such as the availability of critical resources, post-incident reviews and lessons learned, and communication plans for engaging key stakeholders and customers during business disruptions.

Outsourcing and due diligence

Strengthening due diligence in outsourcing arrangements

Survey responses indicate that outsourcing is common across the sector. However, due-diligence processes are often basic and do not fully address several key elements recommended under the DI standard conditions. Strengthening due-diligence practices when selecting external service providers would help ensure that reliance on third parties does not create unmanaged operational vulnerabilities.

Outsourcing oversight

Reviewing outsourcing arrangements and formal agreements

Where outsourcing arrangements exist, agreements should clearly set out expectations for performance monitoring, remedial actions for non-performance, continuity requirements, and other key elements of the arrangement. These outsourcing arrangements should also be reviewed at a frequency that aligns with the level of risk involved to strengthen oversight and accountability.

Technology and information security

Strengthening technology resilience and security practices

Survey responses show a heavy reliance on highly customised technology systems. However, the adoption of recognised information security frameworks and effective monitoring measures to protect these systems remain uncommon. Entities should consider implementing established information security frameworks and strengthening their monitoring and detection capabilities.

Incident management

Improving incident identification and notification readiness

Although processes for identifying and notifying incidents are in place, their effectiveness is not routinely tested. Testing these processes and improving staff awareness would help ensure incidents are identified, escalated and notified in a timely and consistent manner.

We encourage all derivatives issuers to reflect on these findings and consider how the insights and opportunities outlined here can inform their own operational resilience practices. By working together, sharing experiences, and embracing continuous improvement, derivatives issuers can collectively strengthen the resilience of their sector and ultimately New Zealand's financial markets for the benefit of all participants.

Next Steps

We welcome the work done by derivatives issuers to build their operational resilience. As well as supporting well-functioning financial markets, this helps consumers to have confidence that their interests are being looked after and that there are procedures in place to respond to and recover from an event if disruption occurs.

As noted in our 2025 Financial Conduct Report, the FMA is taking steps to deepen our understanding of operational resilience practices and is committed to supporting the sector's ongoing journey. The feedback provided through the survey will shape our future regulatory strategy and initiatives for operational resilience.