FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

JANUARY 2026

Operational resilience thematic: findings and insights – peer-to-peer lending sector

Introduction

In 2025 the Financial Markets Authority – Te Mana Tātai Hokohoko (FMA) surveyed peer-to-peer (P2P) lending service providers as part of our thematic review of operational resilience. We would like to thank all P2P lending providers 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

The P2P sector in New Zealand is on a positive journey 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 P2P lending providers, 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, with investment ranging from $10,000 to $500,000 (representing less than 1% to more than 10% of annual revenue of the entity).
- **Board capabilities**: All respondents have at least one board member with operational resilience expertise, but only a minority provide regular (annual) board training on operational resilience. Most boards receive training 'as needed', which may limit their ability to stay ahead of emerging risks.
- **Risk management**: Risk management frameworks are widely in place, but only some entities have fully embedded these frameworks into day-to-day operations. Self-assessment scores range from 3 to 5, indicating room for more consistent application across the sector.
- **Compliance culture**: Boards and senior management regularly discuss operational resilience, and all respondents have remediation procedures for non-compliance. Scores are high (4 to 5), reflecting a strong compliance culture.
- **Awareness of obligations**: Most boards rate their awareness of operational resilience obligations highly (4 to 5), although understanding of technology and information security requirements is sometimes lower.

Overall governance scores for each entity ranged from 3.5 to 4.7 out of 5

Outsourcing

- **Use of providers**: All respondents rely on external service providers, with some depending heavily on a small number of providers for critical functions.
- **Overseas providers**: Use of overseas providers is limited, but where they are used, entities are aware of the additional risks and regulatory requirements.

- **Due diligence**: Most entities have basic due diligence procedures, but only a few have robust, written processes that cover all key risk areas (e.g. past performance, complaints handling, regulatory protections).
- **Performance monitoring**: Active monitoring of service providers is common, with formal agreements in place that include business continuity and technology requirements. However, the frequency and depth of reviews vary.
- **Formal agreements**: While all respondents have agreements, not all include comprehensive provisions for performance monitoring, termination, and continuity.

Overall outsourcing scores for each entity ranged from 2.9 to 4.2 out of 5.

Incident management and business continuity plans (BCP)

- **Documented BCPs**: All respondents have documented BCPs, but the inclusion of post-incident reviews and lessons learned is inconsistent.
- **Implementation:** Most entities have internal controls, and provide annual BCP training to senior management and, in some cases, frontline staff. A few provide more frequent training.
- **Testing and updates**: Scenario-based testing is common, but not universal. Some entities do not test BCPs regularly or communicate results to the board.
- **Compliance knowledge**: Self-assessment scores are generally high, but some entities identify limited resources as a challenge for BCP development and maintenance.

Overall incident management and BCP scores for each entity ranged from 3.4 to 4.5 out of 5.

Technology and information security

- **System complexity**: Most entities rely on highly customised technology systems, with some still dependent on legacy systems for core operations.
- **Staff capability**: Entities generally have competent staff and invest in training, though one entity reported no recent investment in staff training.
- **Investment in upgrades**: Most entities have recently upgraded their technology systems and cybersecurity, with no adverse impacts reported from underinvestment.
- **Information security frameworks**: Adoption of recognised frameworks (e.g. NIST, ISO/IEC 27001) is limited – only one entity reported using such a framework.
- **Monitoring and detection**: Most entities have real-time or near real-time monitoring, but a few still rely on manual processes.
- **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 3.1 to 4.0 out of 5.

Incident notification

- **Materiality criteria**: All respondents use clear criteria (e.g. customer impact, cost, regulatory consequences) to determine incident materiality, but effectiveness of decision-making processes varies.
- **Identification procedures**: Most entities have established procedures and provide staff training, although some have not tested the effectiveness of these procedures.
- **Knowledge of requirements:** While self-assessment scores are generally high across the group, there is some variation in this area.

Overall incident notification scores for each entity ranged from 2.5 to 4.7 out of 5.

Overall assessment

Sector maturity

Although we have not independently verified participant responses, the survey indicates that most peer-to-peer lenders believe they perform well across the assessed areas. Findings suggest the sector has built a solid foundation in operational resilience, with frameworks and processes in place. This demonstrates good awareness of the importance of being resilient to disruptions and taking proactive steps to mitigate related risks. Based on the survey results the FMA believe the areas requiring further attention and improvement are outlined below.

Opportunities for Improvement

Ongoing board and staff development
Regular training will help boards and teams stay ahead of emerging risks and evolving best practice.

Embedding long-term strategies
Developing, maintaining and embedding forward-looking operational resilience strategies and risk management frameworks will support sustainable growth and adaptability.

Enhancing due diligence and performance monitoring
Strengthening processes for selecting and reviewing service providers plus ongoing performance monitoring will further safeguard critical operations.

Continuous BCP improvement
Regular testing, updates, and lessons learned from real events will ensure BCPs remain effective and relevant. Ongoing board and staff training will ensure successful implementation.

Adopting recognised frameworks
Exploring and implementing established information security frameworks can help align practices with global standards and sector expectations.

Strengthening monitoring capabilities
Investing in real-time monitoring and automated alerts will enhance responsiveness to cyber threats and operational risks.

Incident identification and notification
Robust processes for timely incident identification and notification will help with appropriate escalation and incident response. The effectiveness of these processes should be tested.

We encourage all P2P lending providers to reflect on these findings and consider how the insights and opportunities outlined here can inform their own operational resilience journey. By embracing continuous improvement, prioritising those areas that need the most attention or investment in order to increase operational resilience maturity, and sharing experiences, P2P lending providers 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 P2P lending providers to build their operational resilience. This work, together with ongoing improvements in those areas where opportunities remain to increase operational resilience maturity, will support well-functioning financial markets and help 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.