FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

JULY 2026

Operational resilience thematic: findings and insights – insurance

Foreword

Operational resilience is fundamental to maintaining trust and confidence in New Zealand's financial markets. As the operating environment becomes increasingly complex, it is important that insurers are well positioned to respond to and recover from disruptions in a way that protects customers and supports market integrity.

This thematic review provides insights into the sector's current level of operational resilience maturity, based on information shared by participating insurers. While these insights have not been independently verified, they offer a useful perspective on how insurers view their current position and highlight areas where further focus is needed.

The findings suggest that the operational resilience of the insurance sector is still developing. While many insurers reported having frameworks, policies, and business continuity arrangements in place, the overall picture is one of uneven maturity. In several areas, there appears to be reliance on the existence of arrangements and policies, rather than clear evidence that these are consistently robust, well tested and effective in practice. We also observed that self-assessments do not always fully align with the underlying vulnerabilities and gaps identified through the survey.

These observations are consistent with themes identified through our broader supervisory work. In particular, governance, outsourcing, and technology resilience continue to present challenges across the sector. For example, heavy reliance on outsourced and often offshore providers is not matched by consistently strong contractual protections, regular review or credible exit readiness. Similarly, reliance on legacy systems and highly customised technology environments introduces risks that may constrain an insurer's ability to respond effectively to significant disruption. Advancements in frontier AI are likely to amplify these, increasing both the speed at which they can be exploited and the potential scale of operational disruption.

Taken together, the findings through the survey and our supervisory work indicate that, for many insurers, progress in operational resilience has been stronger at a policy level than in operational execution. There remains a need to further embed resilience practices in a consistent manner, supported by effective governance and clear accountability.

We expect insurers to continue strengthening their operational resilience capabilities and to address the areas identified in this review. Doing so will support the sector's ability to respond to disruption and contribute to financial markets that deliver reliable, fair and resilient outcomes for New Zealanders.

Michael Hewes

Director - Deposit Taking, Insurance and Advice

Introduction

In 2026 the Financial Markets Authority – Te Mana Tātai Hokohoko (FMA) surveyed insurers as part of our thematic review of operational resilience. We would like to thank all insurers 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 thematic survey was issued to all insurers covered by the Conduct of Financial Institutions regime on 3 February 2026. Responses were received by 67% of the sector. The responses indicated a broadly positive level of engagement and progress toward operational maturity.

This document highlights the sector's self-identified strengths, acknowledges areas for further development, and provides practical and supportive recommendations. The FMA is committed to working alongside insurers, giving guidance and fostering a collaborative environment where good practice can be shared.

Governance

- **Financial resources**: All respondents indicated that they believe they have sufficient financial resources to invest in operational resilience and technology systems. While the scale of investment varies significantly across the sector (responses indicated investment ranged between less than 1% and more than 10% of annual revenue), 48% of respondents reported that their investment in operational resilience and technology systems is between 2-5% of their annual revenue.
- **Board capabilities:** Most respondents indicated that all board members have operational resilience expertise, with a small proportion (16%) noting that at least one board member has this expertise. Despite this reported capability, ongoing development appears limited, raising concerns about the board's ability to effectively oversee the evolving landscape of operational resilience, technology risk and third-party dependencies. Notably, 77% of respondents do not provide regular operational resilience training to board members and training is predominantly ad hoc.
- **Operational resilience strategy:** Fewer than half of respondents reported having a long-term operational resilience strategy in place. A significant proportion (42%) do not have a standalone operational resilience strategy, relying instead on a collection of related policies (e.g. business continuity, technology, information and outsourcing) to collectively address resilience objectives. A small proportion (13%) indicated that no strategy exists or that one is still under discussion. This raises concern that resilience efforts are likely reactive and fragmented rather than outcomes-focused and forward looking.
- **Risk management framework:** The results suggest that operational resilience risk management frameworks are largely established across the sector, with all entities reporting frameworks are in place and 87% of respondents rating their frameworks as 4 or 5 out of 5 for appropriateness and effectiveness. 10% of respondents indicated that the risk management frameworks are not yet sufficiently embedded into their organisations. This raises concerns regarding gaps in the consistent and effective application of these frameworks across decision-making, frontline processes and day-to-day behaviours.
- **Compliance culture:** Survey responses indicated a strong culture of compliance with operational resilience requirements. 84% of respondents reported that boards and senior management regularly discuss operational resilience. In addition, 97% of respondents indicated that remediation procedures are in place to address non-compliance with operational resilience requirements.

  Self-assessment results relating to board support for establishing a strong compliance culture were also high, with 94% of respondents assigning a rating of 4 or 5 out of 5. This suggests a high level of confidence among respondents in the board's support for fostering a culture of compliance.
- **Awareness of obligations:** Survey results suggest that respondents generally consider their boards and senior management to have a good understanding of the key operational resilience requirements outlined in the Standard Conditions for financial institution licences (**FI standard conditions**). More than 80% of respondents rated their boards or senior management's understanding of these requirements at 4 or 5 out of 5, indicating a high level of self-assessed awareness across the sample.

Overall, governance scores for each entity ranged from 3.2 to 4.9 out of 5.

Outsourcing

- **Use of providers:** Over 90% of respondents reported outsourcing key functions to external service providers, underscoring the importance of third-party service providers to operational resilience. Among

those with outsourced arrangements, the most commonly outsourced areas are critical technology systems (61%) and the support functions for those systems (64%). These services were generally regarded as easier to transition between providers, reflecting the relatively strong availability of alternative providers in the market. In contrast, the availability of providers for customer information/data and cyber-security functions is moderate, with only 18% of respondents indicating that there are many alternative providers in these areas.

Respondents who outsourced key business functions reported a significant reliance on external service providers for the delivery of these functions. 75% of respondents rated their reliance at 4 or 5 out of 5. This indicates that operational resilience outcomes for many firms in the sector are closely tied to the continued performance, availability and resilience of third-party providers.

- **Overseas providers**: A significant proportion of respondents (71%) reported relying on overseas-based providers to deliver key functions. Respondents generally expressed confidence in these providers' capability to meet regulatory requirements, suggesting a high level of trust in their cross-border service arrangements.
- **Performance monitoring**: Most respondents (82%) indicated that they actively monitor their outsourced arrangements and review provider performance. A small proportion (10%) indicated that they monitor performance on an ad hoc basis, typically only when information suggests potential issues.
- **Due diligence**: The majority of respondents (97%) reported having written due diligence procedures in place for outsourcing arrangements. While most (83%) described these procedures as robust, a proportion (17%) indicated that their procedures are more basic.

  The survey indicates that during the external service provider selection process, some respondents do not assess all key matters required under the FI standard conditions 4 – Outsourcing when conducting due diligence on proposed outsourcing arrangements. In addition, some respondents reported assessing a broader range of factors including privacy impacts, operational costs, corporate structure and financial viability, as well as the providers' ability to deliver regular reporting.
- **Formal agreements**: While respondents with outsourcing arrangements have formal agreements in place, many agreements do not include comprehensive provisions for performance monitoring, remedial actions for non-performance, or procedures for terminating contracted services, as is expected to support compliance with FI standard conditions 4 - Outsourcing. Without these contractual levers, firms may have limited ability to respond effectively to provider failures or service disruptions.

  13% of respondents reported that outsourced arrangements are reviewed only at renewal, which does not align with the risk-appropriate frequency requirement of the FI standard conditions 4 - Outsourcing.

Overall outsourcing scores for each entity ranged from 3.1 to 5.0 out of 5.

Incident management and business continuity plans (BCP)

- **Documented BCPs**: All respondents reported having documented BCPs, with 97% of respondents indicating that their BCPs incorporate key components required by FI standard conditions 5 – Business continuity and technology systems. 9% of respondents did not include outsource arrangements in their BCPs as is expected to ensure compliance with FI standard conditions 5.

  Limited resources were noted as an area of challenge by some firms in relation to developing their BCPs.

When self-assessing the appropriateness of their organisations' BCPs, most respondents (87%) rated them as 4 or 5 out of 5, indicating generally high levels of confidence in BCP design.

- **Implementation:** All respondents reported having internal controls in place to support the implementation of BCP procedures. However, only 71% of respondents have verified the effectiveness of the internal controls.

  65% of respondents have previously activated their BCPs in response to a disruption, out of which 95% highly rated (4 or 5 out of 5) the effectiveness of their BCPs.

  Training practices varied across organisational levels. While 90% of respondents provide training to senior management responsible for executing BCP procedures during a disruption, only 42% provide training to board members and 61% provide training to frontline staff. Training is not consistently delivered on a regular basis. Among respondents that provide training, only a portion deliver it on an annual basis: 69% for board members, 79% for senior management, and 53% for frontline staff.

- **Testing and updates**: 97% of respondents reported that they conducted BCP testing using scenario walkthroughs. Of these, 90% of respondents confirmed that their testing scenarios were developed primarily based on their organisation's exposure to potential disruptions, followed by input from cross-functional teams and subject matter experts within the organisation (65%), and the use of historical incidents (58%). Only 6% of respondents reported using external expertise to support the design and implementation of their testing scenarios.

  All respondents who conducted BCP testing reported that testing results were communicated to boards or senior management. Of these respondents, 60% indicated that boards or senior management reviewed and approved the results, and 53% reported that boards or senior management provided further direction on remediation actions. However, 13% of respondents indicated that no actions were taken following the communication of testing results, suggesting that identified issues may not always be followed by appropriate remediation.

  Among respondents conducting BCP testing, changes to business locations (97%), structure (100%), and operations (100%) were identified as triggers for updating BCPs, in addition to gaps identified through testing.

- **Compliance knowledge**: The survey results indicate that respondents generally perceive compliance with business continuity and technology system requirements as manageable. Most ratings fell between moderate (3 out of 5) and easy (5 out of 5), suggesting that requirements are considered achievable, although some respondents indicated that additional support may be beneficial. A small proportion of respondents (3%) reported significant challenges in complying with these requirements.

Overall incident management and BCP scores for each entity ranged from 3.0 to 4.8 out of 5.

Technology and information security

- **System complexity**: All respondents indicated that they have a significant reliance on critical technology systems and reported that these have been specifically tailored to their organisations' needs (more than 90% stating that the level of customisation is moderate to significant). The significant reliance on critical technology systems indicates that technology resilience is a central driver of overall operational resilience outcomes for the sector.

  Over 70% of respondents reported that it would be difficult to replace their critical technology systems (35% of respondents rated the difficulties as 4 out of 5, and 42% of respondents rated the difficulties as 5 out of 5). Respondents identified several key challenges contributing to this complexity, including the

significant investment and resources required to replace highly customised systems, the difficulty of replicating existing functionality, incompatibility between modern platforms and legacy insurance policies, challenges integrating systems within global operating models and the limited availability of suitable vendors in the market.

74% of respondents reported using legacy systems (technology systems that are more than 10 years old) for core operations. Out of these respondents, 43% indicated that more than 30% of their functions rely on legacy systems, while the remaining respondents reported lower levels of reliance. This level of dependency presents a heightened risk where legacy infrastructure may materially constrain operational resilience and limit the entity's responsiveness to evolving risks.

- **Staff capability**: 77% of respondents believe they have an adequate number of staff capable of maintaining their critical technology systems. For some respondents, this relies on external service providers rather than internal staff members, indicating limited in-house capability for maintaining critical technology systems. At least one insurer reported a key-person-risk associated with its legacy policy system. 87% of respondents indicated that they have invested in staff training and expressed confidence in the sufficiency of this investment.
- **Investment in upgrades**: 39% of respondents indicated that upgrades to their critical technology systems and cyber security are conducted on a regular or ongoing basis, while 54% of respondents reported that upgrades were carried out within the past two years.

  The survey indicates that most respondents have made sustained investments in upgrading critical technology systems, with a strong focus on modernisation, cloud migration, and enhanced cyber security. Common initiatives include replacement of legacy policy administration platforms with modern core systems, migration to cloud and implementation of stronger authentication controls such as multi-factor authentication. Respondents also reported upgrades to security infrastructure, including web application firewalls, endpoint and server protection, Security Information and Event Management (SIEM) tooling, and ongoing patch and vulnerability management. While the scale and timing of upgrades vary, the overall approach favours continuous incremental improvements.

  Insurers reported no adverse impacts resulting from underinvestment in critical technology or cyber security in the past 12 months.
- **Information security frameworks**: 90% of respondents indicated using a recognised information security framework. Of these respondents, 79% reported using National Institute of Standards and Technology (NIST) cybersecurity framework, ISO 27001 and CIS (v8), while others used alternative frameworks.
- **Monitoring and detection**: All respondents reported having measures in place to monitor and detect activity that could impact operational resilience of their critical technology systems. 94% of respondents indicated that information is collected in real-time or near real-time.

  Most respondents rely on 24/7 monitoring through Security Operations Centres, underpinned by SIEM capabilities and defined alerting and escalation processes. Monitoring commonly covers networks, devices, internal activities, internal control procedures, credential theft, brand security, portal and web traffic, and cloud services. Real-time monitoring capabilities are frequently augmented through third-party managed services or outsourced monitoring platforms to enhance visibility and efficiency in detecting anomalies.

  Respondents expressed high confidence in the effectiveness of these monitoring and detection measures.

- **Customer data protection**: 94% of respondents reported storing large volumes of customer personal information and expressed high levels of confidence in their ability to protect customer data.

  The survey indicates that respondents generally protect customers personal information through layered defence and controls, which include access management based on least privilege, multi-factor authentication, encryption of data, data masking and segregation of environments. These technical safeguards are supported by continuous monitoring, data loss prevention, vulnerability management, incident response processes, regular testing and clear policies for data classification and handling.

Overall technology and information security scores for each entity ranged from 2.8 to 4.5 out of 5.

Incident notification

- **Materiality criteria**: All respondents reported using clear criteria to determine incident materiality. Most respondents consider the number of impacted customers, potential regulatory or reputational consequences and potential financial cost of the incident such as transaction losses or remediation costs. In addition, 71% of respondents consider the prominence of the incident. A smaller proportion (23%) reported considering other factors, including impacts on service continuity, staff, incident duration and recovery time. The effectiveness of decision-making process for determining materiality were generally highly rated at 4 or 5 out of 5.
- **Identification procedures**: All respondents reported that established procedures to identify incidents are in place and nearly all respondents (97%) reported providing training to relevant staff. However, 13% of respondents reported that the effectiveness of these procedures has not been tested.
- **Knowledge of requirements:** Survey responses suggest that respondents generally have a strong understanding of the mandatory notification requirements set out in FI standard conditions 5 - Business continuity and technology systems.

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 respondents suggests that most insurers view their operational resilience as being at a moderate to mature level. Findings indicate that while foundational frameworks, policies and processes are generally in place, there is scope to further strengthen capability across key areas—particularly in technology and information security which recorded the lowest maturity score (2.8 out of 5).

The results suggest that operational resilience is not yet consistently embedded across all organisations, with some reliance on the existence of procedures rather than clear evidence that they are robust, regularly tested and effective in practice. Challenges related to legacy systems, complex technology environments, and high level of reliance on outsourcing technology systems highlight areas where resilience settings may be under pressure during significant disruption. Overall, while the sector demonstrates awareness of the importance of resilience and has taken positive steps, further focus is needed to ensure these arrangements are sufficiently mature to support effective response and recovery outcomes.

Some areas where the FMA believes further attention and improvement are needed are outlined below:

Board and staff capability

Strengthening board and senior management engagement

The survey reveals boards generally have access to operational resilience expertise; however, training and discussions on this topic are often informal and ad hoc. Implementing more regular and targeted operational resilience training would help boards and senior management maintain visibility of emerging risks and keep operational resilience knowledge current.

Operational resilience strategy

Establishing a long-term strategy

The survey reveals some entities lack a clearly defined long-term strategy and operational resilience measures are fragmented or not strategically embedded. Entities would benefit from formalising a long-term operational resilience strategy that brings together existing policies on business continuity, technology, information security and outsourcing into a coherent framework. This will strengthen oversight, accountability and preparedness for disruption.

Risk management frameworks

Embedding risk management frameworks

While all respondents reported having risk management frameworks in place, these frameworks were not yet sufficiently embedded in some organisations. Further improvement is needed to strengthen board and senior management commitment to the effective use of risk frameworks, integrate risk management more fully into day-to-day decision-making and core business processes plus promote risk-aware behaviours across the organisation.

Outsourcing and due diligence

Strengthening due diligence

Survey responses indicate a significant reliance on external service providers. However, some due diligence processes are basic and do not fully address key elements recommended under the FI standard conditions 4 - Outsourcing. Strengthening due diligence practices when selecting external service providers would help ensure that reliance on third parties does not create unmanaged operational resilience vulnerabilities.

Outsourcing oversight

Reviewing arrangements and agreements

Given the significant reliance on external service providers, entities should ensure outsourcing agreements clearly define expectations for performance monitoring, escalation and remedial actions for non-performance plus termination procedures. These arrangements should also be reviewed at a frequency that aligns with the level of risk involved to strengthen oversight and accountability.

Business continuity planning (BCP)

Ensuring comprehensive BCP coverage

Survey responses indicate that not all respondents are including outsource arrangements in their BCPs, as is expected to comply with FI standard conditions 5. BCPs should explicitly include provisions for outsourcing arrangements and cover key components such as the availability of critical resources, post-incident reviews and lessons learned, as well as the risk of exposure to disruptive events.

Business continuity planning (BCP)

Improving the effectiveness of business continuity arrangements

While survey responses indicate most respondents conducted BCP scenario tests and communicated the test results to the board, follow-up actions are applied inconsistently. Stronger and more active board engagement with testing outcomes, together with clear and structured BCP implementation training, would help ensure that BCPs remain effective, current and operationally useful.

Technology and information security

Strengthening technology resilience

Survey responses indicate a significant reliance on highly customised technology systems that are difficult to replace. Organisations should improve visibility of system dependencies and failure impacts - plus support this by effective and tested recovery plans. Where possible, this should be supported by deeper in-house expertise. Resilience considerations should also be built into future technology decisions to enhance resilience of complex bespoke systems and strengthen recovery from disruptions.

Legacy system

Managing legacy system reliance

Survey responses indicate a significant proportion of core functions rely on legacy systems. Entities should prioritise modernisation strategies and maintain clear oversight of legacy system exposure. This includes supportability and vendor end-of-life risks. Entities may reduce transformation risk by pursuing phased upgrades rather than large-scale replacements, while maintaining contingency plans to ensure service continuity.

Incident management

Improving incident identification and notification readiness

Although survey responses indicate 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 insurers 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, insurers can collectively strengthen the resilience of their sector and ultimately New Zealand's financial markets for the benefit of all participants.

Next steps

We appreciate insurers' ongoing efforts to strengthen 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.