Operational resilience

From regulatory obligation to strategic advantage

A KPMG perspective for New Zealand's regulated financial services sector



KPMG. Make the Difference.

What's shaping operational resilience

01

Operational resilience has shifted from a back-office compliance task to a board-level test of trust – regulators now expect regulated entities to prove, not just assert, that they can continue to provide products and critical services to customers through periods of disruption.

02

New Zealand's regulatory landscape is converging fast: the Reserve Bank of New Zealand (RBNZ's) Deposit Takers Act (DTA) standards (effective from Dec 2028) will look to replace BS11 and Open Bank Resolution (OBR) for banks, while a parallel Insurance Prudential Supervision Act (IPSA) reform is bringing similar standard-making powers to insurers.

03

The FMA's July 2026 insurance thematic review shows the sector is stronger on paper than in practice – 77% of boards get no regular resilience training, and only 6% of testing draws on external challenge. This is not unique to insurance, with the FMA's wider thematic work pointing to similar execution gaps across financial services.

04

The UK's move to directly regulate cloud providers as "Critical Third Parties" signals where global regulatory attention may head next – NZ has no equivalent regime today, but the underlying concentration risk is real.

05

Technology platforms are coming to the market to help regulated entities map and monitor resilience – but they cannot substitute for the harder upfront work of defining services, testing tolerances and embedding genuine accountability.

06

The task ahead differs by regulatory pathway: deposit takers must reconcile BS11 evidence into new DTA registers; insurers need to prepare for standards that do not yet exist; and investment managers and other market services licensees must evidence compliance with the FMA's already-live business continuity, critical technology systems and material incident notification expectations. Operational resilience is therefore a regulated financial services issue—not only a bank and insurer issue.

A regulatory landscape in motion

New Zealand's regulators are sharpening their expectations of operational resilience across licensed financial services, in step with international peers rather than in isolation.

The common direction is clear: providers should be able to identify the services that matter most to customers, investors and market integrity; understand the people, technology, data and third parties that support them; and demonstrate that those critical service providers and services can continue or recover through disruption. The precise obligations differ by licence type and regulatory mandate, but the underlying focus on preparedness, governance, testing and evidence increasingly cuts across the sector. It is no longer whether a service provider has a resilience plan, but whether that plan is proven to work when it is needed.



Customers expect critical services to keep running through disruption, and regulators are increasingly looking for evidence that they will.

The Financial Markets Authority – Te Mana Tātai Hokohoko (FMA)

applies this expectation broadly across licensed market services. Most market services licensees are assessed against relevant business continuity and critical technology standards and must notify the FMA of material disruption events. From 1 July 2024, the FMA introduced a specific standard condition requiring certain licensees to maintain appropriate business continuity arrangements and resilient critical technology systems. It applies to discretionary investment management service providers, derivatives issuers, licensed peer-to-peer lending and crowdfunding providers, and managers of registered managed investment schemes other than restricted schemes. Alongside the conditions applying to licensed financial institutions, this means **operational resilience is already relevant across banking, insurance, capital markets and investment management.** The FMA's recent completed thematic review, published in July 2026, examined insurers and identified gaps between documented arrangements and operational execution, particularly in board training, third-party oversight and testing. Its rolling thematic programme includes **Peer-to-Peer lending sector, Crowdfunding service providers, Derivatives issuers sector**, **Discretionary investment management service sector and managed investment scheme managers** in 2026/27, reinforcing that resilience is not confined to prudentially regulated entities.

The Reserve Bank of New Zealand Te Pūtea Matua (RBNZ)

is, in parallel, embedding operational resilience more directly. For deposit takers, the third and final tranche of DTA standards includes an exposure draft **Operational Resilience Standard 2027.** The standard covers operational risk, critical operations and tolerance levels, ICT risk, material service providers, business continuity and board accountability, with requirements applied proportionately across deposit taker groups. For insurers, the exposure draft **Insurance (Prudential Supervision) Amendment Bill** would significantly expand RBNZ's standard-setting powers for risk management, business continuity and recovery planning, creating a future pathway broadly aligned with the DTA. The Bill is not expected before Parliament until 2027, with standards from 2028, so this remains a direction of travel rather than a current obligation.

In addition, October 2026 joint supervisory expectations from RBNZ and the FMA on cyber risk associated with frontier AI reinforce this direction. The regulators expect entities to maintain strong cyber fundamentals, effective board and senior management oversight, visibility of third-party and concentration risks, and incident response and recovery arrangements tested against severe but plausible scenarios. These expectations build on existing obligations rather than creating a separate cyber resilience regime, and both regulators have signalled that this will remain an active supervisory focus.

Taken together, these developments create related but distinct regulatory pathways. **RBNZ's prudential framework is becoming more prescriptive** for deposit takers and insurers, using concepts such as critical operations, tolerance levels and material service providers. The FMA's framework is already live across a wider group of licensees and emphasises proportionate business continuity arrangements, resilient critical technology systems, customer and investor impacts, and prompt notification of material incidents. For those regulated by both RBNZ and FMA, the regulatory driver may differ, but the operational response should be coherent: one resilience capability that can be scaled to the regulated entity's services, risks and applicable obligations.

For all licensed providers, resilience starts with identifying the customer, investor or market services that need to remain available through disruption. What is critical will differ by sector and business model, but the principle is the same: understand what must keep working, what it depends on, and whether those dependencies can withstand disruption.

What needs to keep working?

Critical services will differ by sector and business model, for example:

Banking & payments
Payments and access to deposits

Insurance
Claims handling

Funds & investment
Trading, valuation and unit pricing, contributions and withdrawals

Across sectors
Registry, reporting and digital access

What does it depend on?

Map the resources supporting each critical service, for example:

People, data & technology

Specialist third parties
Custodians, supervisors, administrators, registries and investment platforms

Technology & group providers
Cloud and offshore/ group services

Can your critical services withstand disruption?

Test the service and its dependencies, with credible contingency and exit arrangements and evidence that they work.

Internationally, the models vary but the objectives are converging

New Zealand's evolving approach reflects a wider global shift towards stronger governance, **clearly defined tolerances for disruption** and evidence that critical services can continue when things go wrong.



Canada

Canada's Office of the Superintendent of Financial Institutions (OSFI) E-21 - Operational Risk Management Resilience (effective September 2026) is similar.



Europe

The EU's Digital Operational Resilience Act (DORA), applicable since January 2025, takes a more ICT-specific approach to strengthening digital operational resilience across financial entities.



United Kingdom

The UK's Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) combined operational resilience regimes (effective March 2025) focus on important business services and impact tolerances,



Australia

The Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 230 (fully in force since July 2026) is the most integrated model, combining operational risk, business continuity, service-provider risk and governance in one standard for banks, insurers and super funds.

Whatever the architecture or terminology, whether "critical operations", "important business services" or "critical functions", regulated entities everywhere are expected to: identify the operations that matter most to customers; map the people, technology, data and suppliers behind them; set and test tolerance levels for disruption; rehearse recovery through severe-but-plausible scenarios; and evidence genuine governance accountability, not just documentation.

For New Zealand organisations operating across borders or benchmarking against an Australian parent, this convergence puts them at an advantage – one well-built resilience capability that can satisfy the FMA, RBNZ's DTA and Insurance (Prudential Supervision) Act (IPSA) standards, and APRA's CPS 230 simultaneously.

New Zealand's legacy landscape: From overlapping regimes to a converged DTA architecture

Before the DTA, New Zealand's largest banks navigated four overlapping regimes.

These all covered similar ground across critical operations, service-provider risk, business continuity and board accountability, all through different legal mechanisms and terminology:

- BS11 (RBNZ's bank outsourcing policy)
- OBR (RBNZ's Open Bank Resolution regime)
- APRA's CPS 230 (for any New Zealand entity in an APRA group)
- FMA's Conduct of Financial Institutions (CoFI) standard conditions (conduct-focused business continuity for all financial institutions).

KPMG's 2024 analysis, **"Navigating Resilience and Resolution,"** found that reconciling them was less about understanding any one regime in isolation, and more about mapping which regulation applied to which underlying business process.

The DTA is now resolving this fragmentation for deposit takers, not by repealing BS11 and OBR, but by converting both into formal DTA standards aligned with the new Operational Resilience Standard. The following table summarises what changes, and what doesn't:

For banks already compliant with BS11, this is a genuine but manageable transition: much of the existing due diligence and testing evidence can be repurposed, but banks will need to reconcile their BS11 Compendium against the broader DTA Register, extend beyond outsourcing to the full concept of critical operations, and prepare for a higher evidentiary bar as RBNZ moves from non-objection to formal approval. The practical lesson, consistent with our 2024 analysis, is the same for insurers watching the IPSA trajectory: build one integrated capability that can flex across whichever regime applies, rather than maintaining siloed compliance efforts for each.

Legacy regime	Current basis	Applies to	What happens under the DTA
BS11 – Outsourcing Policy for Registered Banks	RBNZ conditions of registration under the Reserve Bank of New Zealand Act 1989	Large registered banks (liabilities (net of related party balances) of $10 billion or more)	**Intended to be replaced by the Deposit Takers (Outsourcing) Standard 2027 once the DTA fully commences (1 December 2028).** **Key changes:** • the Compendium becomes the Register of Critical Operations and Material Service Providers; • "outsourcing arrangement" becomes "material service provider (MSP) arrangement"; • the non-objection process becomes a formal RBNZ approval regime, raising the evidentiary bar; • scope narrows from banks with net liabilities ≥$10bn to Group 1 deposit takers (assets >$100bn); and • "statutory management" becomes "resolution".
OBR – Open Bank Resolution	RBNZ policy and conditions of registration	Registered banks	**Evolving into the Continuity of Access to Deposits (CoAD) Standard, part of the DTA's Crisis Preparedness package.** Exposure drafts expected 2027; Standard issued late 2028 – likely later than the Operational Resilience and Outsourcing Standards (due 31 May 2027).
APRA CPS 230 – Operational Risk Management	APRA prudential standard	Any NZ-incorporated entity within an APRA-regulated group	**Unaffected by the DTA – continues to apply directly and in parallel.** RBNZ's Operational Resilience Standard is best seen as a localised, less prescriptive domestic counterpart, built on the same three objectives: managing operational risk, maintaining critical operations, and managing service-provider risk.
CoFI / Standard Conditions for Financial Institution Licences	FMA standard conditions under the Financial Markets Conduct Act 2013	All financial institutions holding a market services licence, including banks and insurers	**Unaffected by the DTA.** This is a separate, conduct-focused regime under different legislation and a different regulator. Deposit takers must continue complying with both regimes in parallel; neither supersedes the other.

Beyond the regulated firm: Regulators turning to the infrastructure underneath

A further international development signals where the conversation may be heading next. On 10 July 2026, HM Treasury formally designated four global cloud and technology providers as Critical Third Parties (CTPs) to the UK financial system, with joint Bank of England (BoE)/PRA/FCA oversight beginning three days later – the first real-world use of powers dormant since 2024.

The rationale is concentration risk: a 2024 BoE/FCA survey found over 65% of UK financial institutions rely on the same small group of hyperscale cloud providers, meaning a single provider's disruption could cascade across the sector. The regime is additive, not a replacement, regulated entities retain full third-party risk responsibility, and further providers may be designated over time.

New Zealand has a narrower precedent in Financial Markets Infrastructure (FMI) Standard 17B (Critical Service Providers), which since March 2024 has required operators of designated financial market infrastructures to manage risks arising from critical service providers. However, the standard operates through the FMI operator rather than imposing direct RBNZ or FMA oversight on the providers themselves. New Zealand therefore has no equivalent to the UK's economy-wide critical third-party regime for banks, insurers and other regulated financial services providers. Given the sector's reliance on a concentrated group of offshore cloud and technology providers, this remains an area worth watching.

What the evidence tells us

The FMA's July 2026 insurance thematic review on operational resilience, which received responses from **67% of the sector,** shows progress has been considerably stronger at the level of policy than in operational execution. While all respondents felt adequately resourced:

77% provide no regular board resilience training;

only a slim majority have a standalone resilience strategy

42% rely on a patchwork of related policies

13% have none at all;

over **90%** outsource key functions; and 71% rely on overseas providers, often without matching contractual protection or exit planning; and

74% rely on legacy systems over a decade old; and testing remains desktop-heavy, with only 6% using external challenge and 13% taking no action after issues were identified.

A fairly sobering list of stats.

These findings mirror KPMG's international experience. As UK regulated entities approached the March 2025 PRA/FCA combined regime compliance deadline, common weaknesses included incomplete asset registers, programme-led rather than embedded resilience, poor use of existing risk data, limited third- and fourth-party visibility, desktop-heavy testing, and weak integration with business continuity and crisis management. KPMG UK's published analysis, **Making Society More Resilient: Navigating Disruption with Confidence (April 2026)**, provides broader corroboration, highlighting technological and supply-chain interdependence, cascading disruption and the need to treat operational resilience as a board-level strategic priority.

How the market is responding

As expectations mature, technology and advisory providers globally are moving quickly to productise operational resilience management, bringing cloud-based platforms that map business processes, technology and third-party dependencies into a single real-time view, or tools that set tolerance levels and surface vulnerabilities from one source of truth.

The shared thesis: the barrier to good resilience is less about knowing what "good" looks like, and more about the sheer difficulty of maintaining an accurate, current picture of services and dependencies manually – a pain point the FMA's own thematic review echoes directly.

KPMG's 2026 Global CCO Survey (responses from 725 Chief Ethics and Compliance Officers (CCO)) reinforces how central this has become globally: 75% of Chief Ethics and Compliance Officers surveyed are prioritising further cybersecurity investment, 77% cite data analytics as a key driver, and resilience is increasingly a cross-functional discipline rather than a specialist silo.

But boards should ask a harder question of any technology-led offer: a platform can surface a vulnerability faster than a spreadsheet, but it cannot substitute for genuinely knowing which services matter, having tested the ability to keep them running, or having a culture that acts on what the data reveals.

The FMA's own findings, high self-assessed confidence sitting alongside limited board training and desktop-only testing, suggest New Zealand's real gap today is not a lack of dashboards, but a lack of embedded ownership and evidenced discipline. Any technology investment is only as good as the operating model wrapped around it. Defining services, testing tolerances and embedding genuine accountability should precede any investment in operational resilience tooling.



From “Do we have a plan?” to “Can we actually cope?” – A practical path forward

This convergence is prompting a shift in how the best boards talk about resilience: away from “do we have a business continuity plan, signed off?” and toward “have we genuinely tested our ability to keep critical services running, and can we prove it to a regulator and our customers?”.

A plan that exists only on paper ticks one box. However, a capability that has been tested through a live incident or a genuinely challenging scenario is fundamentally more valuable, and increasingly a source of competitive advantage, because it builds customer trust and gives regulated entities the confidence to pursue growth from a position of strength.

Building this capability is a multi-year journey, but organisations don't need to start from a blank page. The most effective approach repurposes what regulated entities already have (risk frameworks, BCM plans, Third Party Risk Management (TPRM) standards, asset registers) through a customer-centric, service-based lens. In practice this means: an honest maturity assessment against the relevant standard; pivoting to a service-led view of the handful of operations that matter most; mapping the dependencies behind them; setting and genuinely testing tolerance levels; strengthening board reporting to be evidence-based rather than assurance-by-existence; and treating resilience as an ongoing accountability, not a programme with an end date.

Common implementation challenges seen in New Zealand and abroad:

- Incomplete mapping and legacy technology: gaps in service, process and data asset registers, particularly where systems are highly customised or ageing.
- Resilience funded as a project, instead of an embedded capability and culture: requirements from different regimes are addressed separately, without the ongoing investment in people, culture, process and technology to embed resilience as business-as-usual.
- Third and fourth-party blind spots, including:
  - limited visibility of how providers’ use of AI could introduce or amplify cyber threats,
  - unmanaged concentration risk: heavy reliance on outsourced and offshore (including cloud) providers, without matching contractual protection, monitoring or exit planning.
- Testing that confirms rather than challenges: desktop-heavy scenario testing with limited independent or external challenge.
- Fragmented frameworks and reporting: operational risk, BCM, TPRM and recovery/resolution planning run as disconnected disciplines with separate data and reporting lines – a pattern reinforced by New Zealand’s historically overlapping regimes (BS11, OBR, CPS 230, CoFI) and now the DTA’s parallel standards.
- Technology ahead of foundations: investing in resilience monitoring platforms before establishing the service definitions, ownership and governance that make such tools valuable.

Key questions for boards and executives



- Can you name your critical or important business services, and what would happen to customers if each failed for an hour, a day or a week?
- Have you genuinely tested tolerance levels for disruption and could you evidence this convincingly to a regulator? What about vulnerable customers?
- How dependent are you on outsourced, offshore and cloud providers, and do your contracts and exit plans reflect the true scale of that dependency?



- When did your board last receive substantive resilience training, and could members articulate your risk appetite for disruption in their own words?
- Are your operational risk, BCM, TPRM and recovery/resolution frameworks harmonised under one critical-operations lens, or run in silos?
- If you're a bank under BS11, have you started thinking through how your existing BS11 Compendium would map against the broader concept of critical operations set out in RBNZ's exposure drafts – so you're not starting from scratch once the Register of Critical Operations and Material Service Providers is finalised?



- If you're an insurer, are you tracking the IPSA Bill's proposed standard-making powers and what a DTA-aligned standard could mean for you?
- If you are an investment manager or other market services licensee, which investor or client services must remain available during disruption, and are trading, valuation, unit pricing, registry, contribution, withdrawal, reporting and client-access processes covered by realistic recovery testing?



- If you are an investment manager, have you mapped and tested dependencies on custodians, supervisors, administrators, registry platforms, cloud providers and offshore group services, including credible contingency and exit arrangements?
- Have your foundational cyber controls, cyber security strategy and risk appetite been reassessed against the increased speed, scale and sophistication of AI-enabled threats, including risks arising through legacy systems and third parties?



- Can your incident governance identify when a disruption or cyber event becomes material, escalate it promptly, and support FMA and RBNZ regulatory notification requirements and supervisory expectations within applicable timeframes, including 72-hour reporting obligations where required?

How KPMG can help

Operational resilience expectations are converging in substance across New Zealand's regulated financial services sector, but the legal drivers, terminology and timelines differ. KPMG draws on a proprietary operational resilience methodology, developed through work with banks, insurers, investment managers and other regulated entities across multiple jurisdictions, to help clients assess where they stand, prioritise the areas of greatest regulatory, investor and customer risk, and build a practical, evidence-based path to resilience.

For deposit takers

We can help you benchmark against RBNZ's emerging Operational Resilience and Outsourcing Standards and help you reconcile your BS11 Compendium and OBR-readiness evidence against the new Register rather than rebuilding from scratch. Assess alignment with APRA's CPS 230 if you report into an Australian parent and continue meeting the FMA's CoFI conditions in parallel.

For insurers

We can help you track and prepare for the IPSA Amendment Bill's proposed standard-making powers ahead of the standards being drafted. We can also help you address the gaps identified in the FMA's July 2026 thematic review, including board capability and training, operational resilience strategy, outsourcing and offshore provider oversight, business continuity testing and remediation, technology resilience, and incident management readiness. We can then benchmark your approach against international frameworks such as APRA CPS 230.

For investment managers and other market services licensees

We can help Managed Investment Scheme (MIS) managers, Discretionary Investment Management Schemes (DIMS) providers and other relevant licensees assess their business continuity and critical technology arrangements against FMA expectations; identify the investor and client services that matter most; map dependencies across custodians, supervisors, administrators, registry and investment platforms and offshore providers; strengthen material-incident assessment and notification procedures; and design testing that reflects plausible disruption to trading, valuation, unit pricing, registry, contributions, withdrawals, reporting and client access.

Across all regulated financial services

We can help map critical or important operations and their dependencies; design genuinely severe-but-plausible scenario testing; harmonise operational risk, BCM, TPRM and recovery/resolution planning under one critical-operations lens; and help you evaluate whether, when and how technology platforms fit your maturity and governance model, so technology follows, rather than substitutes for, the foundational work.

Operational resilience is no longer a question of whether regulators will ask hard questions about an organisation's ability to withstand disruption. It is a question of when they will ask, and whether the answers will be backed by genuine evidence.

Organisations that treat this as an opportunity to build lasting customer trust, rather than simply another regulatory deadline, will be best placed to thrive as the regulatory landscape continues to evolve.

Contact us

For more information.



Malcolm Bruce

Partner
Risk Consulting
KPMG New Zealand
M: +64 217 70693
E: malcolmbruce@kpmg.co.nz



Sarah Pacey

Associate Director
Consulting
KPMG New Zealand
M: +64 27 3149 882
E: sarahpacey@kpmg.co.nz



Damien Barrett

Director
Consulting
KPMG New Zealand
M: +64 27 2616 714
E: damienbarrett@kpmg.co.nz



Sinan Dalgic

Director
Consulting
KPMG New Zealand
M: +64 21 846 949
E: sinandalgic@kpmg.co.nz

©2026 KPMG, a New Zealand Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the author and do not necessarily represent the views and opinions of KPMG, a New Zealand partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

KPMG is a global organisation of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organisation or to one or more member firms collectively.

This publication may incorporate AI-assisted content which has been subject to human review in accordance with KPMG's Trusted AI Framework.