



NEW ZEALAND
CIO INNOVATION
SUMMIT & AWARDS

Sovereign AI In New Zealand: Global Innovation With Local Control

PUBLISHED
January 2026



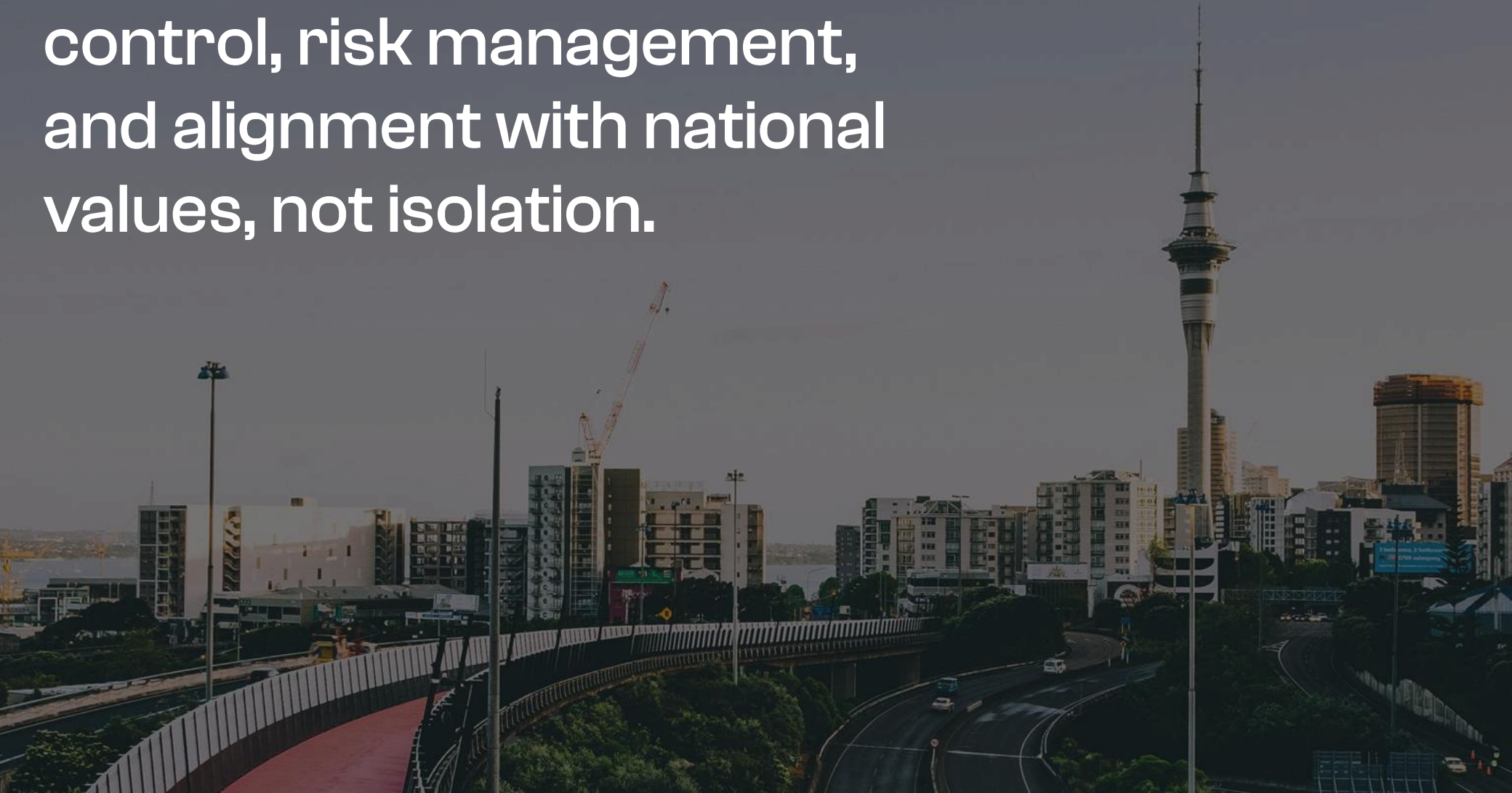
As AI moves into core systems and handles more sensitive data, sovereignty and data governance are becoming board-level concerns.

New Zealand's AI strategy encourages the use of global models, but that introduces real questions around jurisdiction, service continuity, and regulatory control.

In practice, many organisations will need a tiered setup — running some models locally, tuning others in-country, and using global models where it makes sense — to balance performance with compliance and data protection.



AI sovereignty is about local control, risk management, and alignment with national values, not isolation.





AI Sovereignty: Four Areas to Consider

AI sovereignty can be understood across four interconnected layers that define how AI is deployed and governed within a country.

Data Control

How sensitive or culturally significant data is collected, used, shared, and retained.

Operational Control

Whether critical workloads stay on domestic infrastructure and models are adapted locally when it matters.

Governance & Trust

Policies, processes, and guardrails that ensure AI aligns with local regulations, values, and national priorities.

Local Capability

Building domestic skills and institutions to reduce reliance on external providers for critical AI systems.



Māori AI Sovereignty: Cultural Data Control

AI sovereignty also has culturally specific dimensions. For Māori communities, it goes beyond data storage to who controls decisions and how cultural knowledge is used. Organisations must embed these principles into their AI strategies.

Decision Rights and Consent

Defining who can approve the use of Māori data and ensuring consent is enforced through policy and controls.

Cultural IP Protection

Preventing scraping, model training, or commercial reuse of cultural knowledge without explicit permission.

Kaitiakitanga in Controls

Embedding stewardship throughout access controls and data management to ensure data is used appropriately.



Operationalising Sovereignty: Hybrid AI Strategies

With general and Māori sovereignty frameworks in place, organisations must deploy AI in ways that meet these requirements. Hybrid AI deployment lets them uphold sovereignty while tapping into global innovation.



Hybrid AI Architecture

Critical and sensitive workloads run within New Zealand-controlled environments, while lower-risk workloads can use offshore services.



Sovereign Cloud Options

Organisations can select public AI, private AI, or nationally operated environments depending on risk profile.



Resilience & Portability

Multi-model, multi-cloud setups ensure continuity and flexibility while avoiding vendor lock-in.



Strategic Mandates for Technology Leaders





1. Rethinking the Role of Technology

Technology leaders must also orchestrate risk, compliance, and trust across human and AI systems, while managing software. Key areas to focus on:

01

Workload Classification

Identify which AI workloads are high-risk and need to be executed locally, versus lower-risk workloads that can run on global clouds.

02

Portability & Exit Strategies

Avoid vendor lock-in by designing models and infrastructure that can move between providers if regulatory or operational needs change. Containerisation and open-source frameworks make this possible.

03

Vendor Oversight

Go beyond checking where data is stored. How models are trained, who can access model weights, and how providers meet New Zealand's values-based regulatory expectations need to be reviewed.



2. Building Local Capability as Part of Infrastructure

Sovereign AI requires not just the right systems but the right people. Teams need the skills to build, tune, and govern AI locally, ensuring both compliance and performance. Focus areas include:



AgenticOps Teams

Specialists who manage autonomous AI workflows, handle prompt engineering, and fine-tune models to meet local requirements.



Embedded Expertise

Technology experts are embedded directly within business units, providing a controlled “Sovereign Sandbox” where experimentation can occur safely without creating shadow AI on offshore platforms.



Trust & Transparency

IT leaders who can ensure explainability through governance platforms that provide clear, auditable trails of AI decision-making.



3. Following a Structured Framework

Moving from experimentation to enterprise-grade sovereign AI requires structured steps.

IMMEDIATE

Perform a “Sovereignty Audit” of AI systems, pinpointing sensitive or Māori data tied to offshore providers and identifying workloads critical for compliance and operational continuity.

MEDIUM TERM

Create a Hybrid AI Landing Zone. Partner with local infrastructure providers to host critical workloads with low latency, while lower-risk workloads can continue using global resources.

LONG TERM

Embed stewardship into the digital core. Automate data lineage and cultural IP protections to manage Māori and other sensitive data responsibly, shifting from reactive compliance to proactive governance.



Ecosystem Opinion

Geopolitical pressures, export controls, and concentration among a few providers make dependency not just a compliance concern but also a continuity risk. Equally important are local model tuning and governance, with stakeholders demanding trust, transparency, and alignment with New Zealand values.

Tech leaders should focus on classifying AI workloads and data according to risk and implementing a hybrid deployment strategy. Governance and controls need to limit shadow AI while still allowing access to global AI capabilities where appropriate.



NEW ZEALAND

**CIO INNOVATION
SUMMIT & AWARDS**

