FUTURE GOVERNMENT INSTITUTE
Powered by Public Sector Network

CAPABILITIES BEFORE CODE: MATURITY, LEADERSHIP AND IDENTITY IN THE DIGITAL PUBLIC SECTOR

EXECUTIVE SUMMARY | VOL.20 | NEW ZEALAND

VICTORIA UNIVERSITY OF WELLINGTON TE HERENGA WAKA

IN BRIEF

The New Zealand Digital Government Roundtable convened leaders from government, academia, and industry to explore the future of digital transformation and public sector innovation. The session, held under Chatham House rules, centred around three interwoven themes: capability and maturity in digital government, citizen-centric service design, and the development of secure, trustworthy digital infrastructure.

Participants voiced urgency around enhancing digital capability across agencies, citing legacy systems and insufficient investment in foundational technology as persistent barriers. Despite enthusiasm around AI and emerging technologies, discussions underscored that maturity gaps at both organisational and technological levels often stall innovation. Trust frameworks, digital identity infrastructure, and data assurance emerged as critical enablers for more integrated, citizen-driven services.

The roundtable called for co-designed, federated strategies that recognise system-wide interdependencies and build from shared standards. Forward-looking initiatives were highlighted, including safe AI prototyping environments, digital maturity benchmarking, and data infrastructure modernisation. A key takeaway was the importance of aligning digital strategies with decision-making accountability and cultural change, ensuring leadership is equipped to recognise and act on new capabilities. The conversation pointed to an urgent need for agile, collaborative models to overcome structural silos and deliver trusted, high-value digital services.

By **Patrick Joy** | Head of Research & Analysis | **Public Sector Network**

KEY THEMES AND INSIGHTS

DIGITAL MATURITY IS A PREREQUISITE, NOT A BY-PRODUCT

A prevailing theme was that digital maturity must be actively cultivated rather than assumed to emerge organically. Agencies described large capability gaps in their workforces and leadership ranks, limiting their ability to take advantage of technological advances. One participant noted that "people don't even understand the questions they're being asked" about digital strategy, highlighting an education and awareness gap.

Maturity models were proposed as tools to diagnose readiness, guiding technology investments toward outcomes rather than novelty. A tiered framework encompassing organisational maturity, AI readiness, and technological stability was suggested. This approach enables tailored interventions like deploying AI summarisation tools where data infrastructure is strong, but avoiding predictive systems where governance maturity lags.

INVESTMENT PARALYSIS: LEGACY SYSTEMS AND RISK AVERSION

Despite widespread recognition of AI's potential, a pattern of underinvestment was evident. Few AI pilots have matured due to a lack of sustained funding and unclear value metrics. Legacy systems continue to dominate IT budgets, leaving little room for innovation.

Participants noted that small-scale automations in back-office assurance functions show promise, but scalability remains elusive. One official recalled spending tens of thousands of dollars on a process automation yielding marginal gains due to low volume and high complexity. This underscores the need for clear ROI frameworks that factor in organisational scale and readiness.

TRUST, IDENTITY, AND MISSING INFRASTRUCTURE

Digital identity and trust frameworks featured prominently in the discussion. Participants acknowledged that without secure, interoperable identity systems, many citizen-facing innovations would remain aspirational. There was consensus that while privacy remains a core value, the reluctance to pursue national identifiers has created fragmentation. Examples from Denmark and Estonia were raised to illustrate how centralised identifiers can drive service integration. By contrast, New Zealand's patchwork of credentials (e.g., passports, driver's licences, community cards) lacks coherence. Participants called for "assurance levels" to validate identity claims and for government to play a more active role in setting standards.

CITIZEN-CENTRIC DESIGN BEYOND THE BUZZWORD

The roundtable cautioned against tokenistic interpretations of citizen design. True citizen-centricity requires embedded feedback loops, co-creation, and service integration. One speaker described a failed attempt to integrate disability information from health records into service delivery—an example of siloed ownership derailing integration.

Participants highlighted the need for user-controlled platforms that allow citizens to manage their data across services. Generative AI and chat interfaces were seen as potential enablers of better citizen interactions, provided they are built on ethical, inclusive, and accessible design principles.

CHALLENGES AND BARRIERS

STRUCTURAL AND FUNDING CONSTRAINTS

Participants consistently pointed to the limitations of the existing funding models, particularly the siloed nature of vote-based budgeting. These constraints hinder multi-agency collaboration and prevent scaling of pilots beyond proof-of-concept. Despite shared aspirations around integration, agencies struggle to demonstrate joint value under current Treasury rules.

CULTURAL RESISTANCE AND LEADERSHIP GAPS

Digital transformation efforts are often stymied by leadership that lacks digital fluency. There remains an ingrained preference for large, traditional IT projects over agile, iterative approaches. The inability to "stop doing" legacy processes was described as a key inhibitor, with sunk costs and institutional inertia slowing progress.

FRAGMENTATION OF IDENTITY INFRASTRUCTURE

Without a clear mandate or ownership of identity standards, digital services remain fragmented and inconsistent. Agencies are left to navigate identity assurance individually, resulting in duplicated efforts and uneven citizen experiences. Trust frameworks exist in theory but are rarely applied coherently across services.

FUTURE FOCUS AREAS

FEDERATED DIGITAL IDENTITY AND TRUST STANDARDS

Establishing federated identity infrastructure should be a national priority. This includes standardising assurance levels, developing shared credentialing systems, and clarifying data custodianship. Future roundtables could explore models from Scandinavia and the EU to identify lessons for New Zealand's federated context.

AI ASSURANCE AND SAFE PILOTING ENVIRONMENTS

Developing shared AI assurance frameworks will be critical for responsible scaling. Participants supported establishing safe environments for AI prototyping, enabling agencies to test models without risking harm. These environments should be paired with capacity-building efforts focused on ethical design and procurement.

LEADERSHIP CAPABILITY BUILDING AND MATURITY BENCHMARKING

To embed transformation, senior leaders must be equipped with the language, frameworks, and tools of digital governance. Benchmarking maturity across agencies—linked to strategic investment pathways—can help shift funding from reactive to proactive. Leadership capability labs or embedded fellowships were floated.

CITIZEN CO-DESIGN AT SCALE

Scaling citizen engagement requires structural change—not just better surveys. Investment in platforms that support participatory design, particularly for vulnerable or digitally excluded communities, was identified as a key area for future exploration. Ensuring inclusive design becomes embedded in policy and delivery processes is essential.

INNOVATIVE IDEAS AND CASE STUDIES

1. ASSURANCE FUNCTIONS AS AUTOMATION FRONTIERS

Back-office assurance and risk functions were identified as fertile ground for automation. For example, applying AI to summarise complex compliance documentation or flag inconsistencies in financial auditing processes could yield significant efficiency gains. However, these use cases require tightly scoped datasets and high data quality.

2. SAFE AI PROTOTYPING: A 'REGULATORY SANDPIT' APPROACH

One jurisdiction described the creation of an Emerging Technology Advisory Group and a safe prototyping infrastructure where innovations could be trialled before scaling. This regulatory sandpit model enables experimentation with generative AI and other emerging tools in a controlled, evaluative environment.

3. DIGITAL CAPABILITY FRAMEWORKS ANCHORED IN ROLES

Participants advocated for explicit digital capability requirements aligned with professional roles. For instance, information managers should have a baseline understanding of cybersecurity, ethical data use, and AI implications. Embedding such capabilities into job descriptions and performance reviews was proposed as a long-term goal.

4. USER-CONTROLLED DIGITAL SERVICE INTEGRATION

A forward-looking idea involved user-mediated service integration—where individuals could instruct platforms (via AI) to retrieve data from one agency and submit it to another. This vision of "personal APIs" shifts power to citizens while also demanding interoperable infrastructure and clear governance rules.

STRATEGIC OUTCOMES AND RECOMMENDATIONS

IMMEDIATE ACTIONS

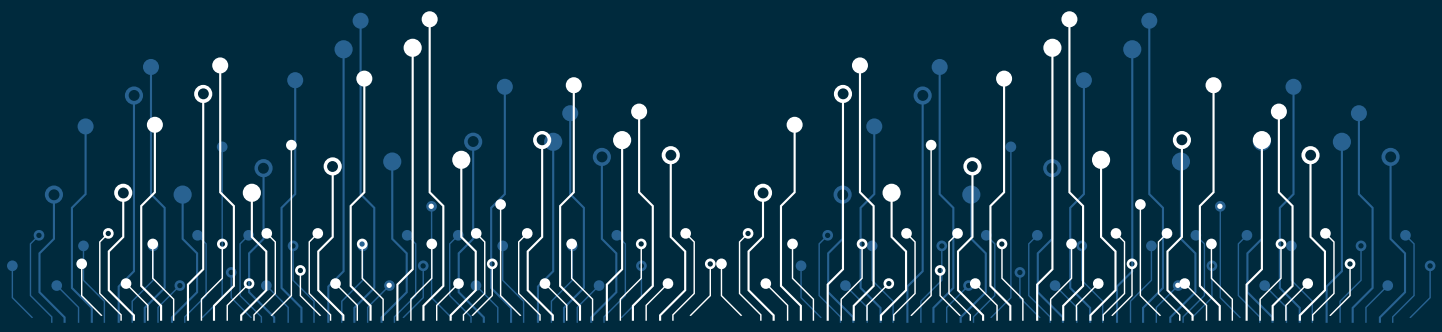
- Develop a shared AI assurance framework with clear principles and thresholds for risk.
- Create safe prototyping environments for emerging technologies within regulatory boundaries.
- Launch targeted leadership development programs to build digital fluency across executive roles.

MEDIUM-TERM GOALS

- Design a federated identity system with defined assurance levels and credential interoperability.
- Build maturity assessment tools to guide investment decisions and track organisational progress.
- Develop shared platforms for citizen co-design and feedback loops.

LONG-TERM VISION

- Shift funding structures toward outcomes-based, cross-agency models that incentivise collaboration.
- Establish national digital standards (identity, data sharing, ethical AI) to underpin service integration.
- Foster a digital government ecosystem where trust, inclusion, and innovation are embedded into public service delivery.



ABOUT THE FUTURE GOVERNMENT INSTITUTE (FGI) RESEARCH COUNCIL

We've been able to engineer a new program antithetical to the classical red tape, administration, and risk-aversion that impedes innovation.

Public Sector Network has recently launched The Future Government Institute (FGI), a global hub for forward-thinking public sector leaders, innovators, and practitioners dedicated to shaping the next era of governance.

Our mission is to empower government professionals with the tools, insights, and networks needed to drive meaningful transformation - https://publicsectornetwork.com/future-government-institute/

Leveraging our extensive connections, we are uniting the sharpest minds from government, academia, and industry via monthly research-driven roundtables, hosted at esteemed national centres of research, courtesy of university partners across Australia and New Zealand.

ABOUT PUBLIC SECTOR NETWORK

Public Sector Network is a research company that represents public sector professionals across Australia, Canada, New Zealand, and the USA. It develops roundtables, seminars, and conferences to suit current areas of interest to government agencies and their suppliers.

PSN's growing community spans across federal, state, and local government departments, healthcare, and education, allowing members to share information, access the latest in government innovation, and engage with other like-minded individuals on a secure and closed-door network.

AUSTRALIA / NEW ZEALAND
P +61 2 9057 9070
E INFO@PUBLICSECTORNETWORK.COM.AU

USA
P +1 (647) 969 4509
E HELLO@PUBLICSECTORNETWORK.COM

CANADA
P +1 (647) 459 8904
E CONTACT@PUBLICSECTORNETWORK.CO

Public Sector Network (Australia) Pty Ltd
ABN - 46 617 870 872 20-40
Meagher Street, Chippendale, Sydney NSW 2008, Australia