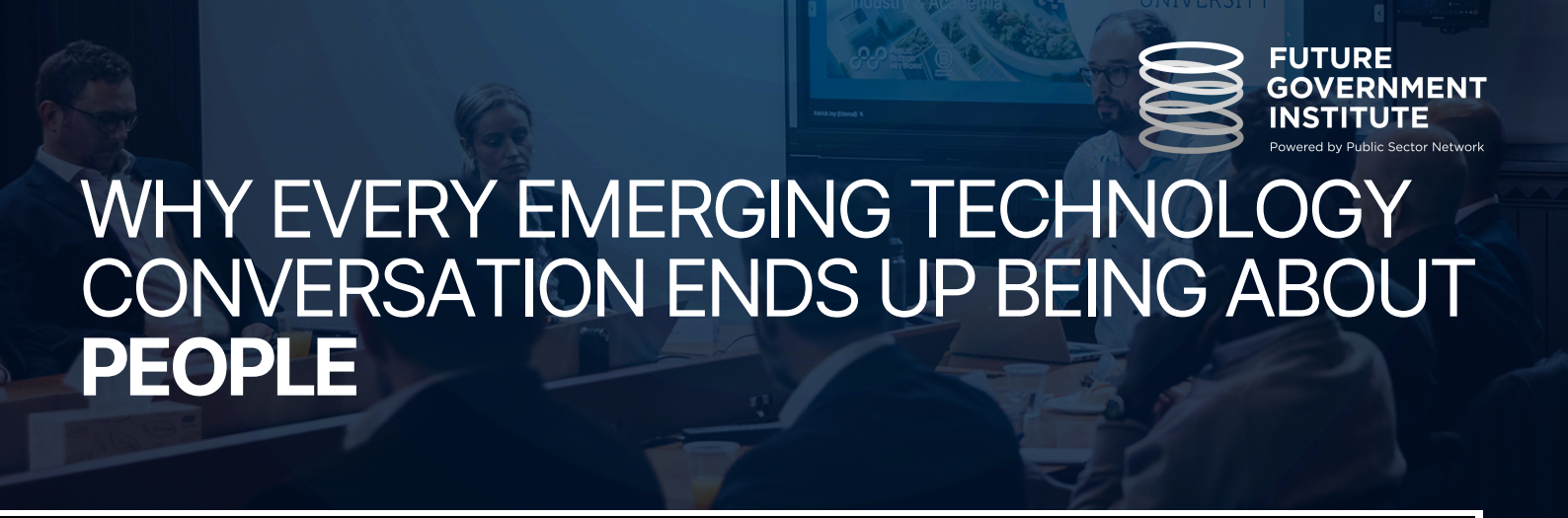


FUTURE GOVERNMENT INSTITUTE
Powered by Public Sector Network

WHY EVERY EMERGING TECHNOLOGY CONVERSATION ENDS UP BEING ABOUT **PEOPLE**

EXECUTIVE SUMMARY | VOL.36 | NEW SOUTH WALES

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

IN BRIEF

The Research Council convened a roundtable focused on how government can adopt emerging technologies with greater speed and confidence, while maintaining trust, accountability and service quality. While the conversation ranged across quantum, digital identity, automation and IoT, participants repeatedly returned to the same conclusion: technology is rarely the constraint. The most persistent blockers are governance, risk appetite, data access, workforce capability and the incentives shaping cross-agency collaboration.

AI and automation were viewed as the dominant near-term lever for productivity, particularly through legacy modernisation, intelligent document processing, triage and booking workflows, and internal knowledge and case management. However, participants noted that "pilot culture" remains a structural failure mode, with many proofs of concept never scaling due to unclear use cases, weak measurement baselines, and governance processes designed to avoid blame rather than enable delivery. Several participants argued for reframing governance as an accelerator, paired with mandatory training and clearer accountability for decisions supported by AI.

Looking forward, the group highlighted four system priorities: building trust and assurance; investing in sovereign-grade data and AI infrastructure; strengthening human agency and inclusion through capability uplift; and redesigning governance to support safe experimentation, contestability, and measurable outcomes for citizens.

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

KEY THEMES AND INSIGHTS

THE FUTURE IS NOT ONE TECHNOLOGY, IT IS A STACK

Participants rejected the idea that emerging technologies can be prioritised as competing "winners". AI, digital identity, sensors and automation were described as mutually reinforcing layers of digital transformation: IoT expands the data surface, AI extracts value and enables decision support, and identity and security become the gatekeepers for trust in a synthetic media world. This framing shifted the question from "Which technology?" to "What capabilities must government build so the stack can be adopted safely and at pace?"

Treating technologies as separate programs leads to fragmented investment and inconsistent risk treatment. A stacked view encourages shared standards, reusable governance, and capability building that travels across use cases.

Agencies should invest in shared foundations (data products, identity, auditability, model governance) rather than funding isolated pilots.

DIGITAL IDENTITY IS BECOMING A FRONTLINE RISK AND SERVICE ENABLER

A strong thread emerged around identity integrity in an era where synthetic content and credential fraud are increasingly accessible. Participants highlighted that faking identity is no longer sophisticated work and that digital services are approaching a point where trust cannot rely on "traditional" signals. Emerging age verification workarounds were cited as an early indicator: if basic verification can be bypassed, government-facing services with financial or legal consequences will be targeted.

Identity underpins eligibility, payments, compliance and trust. If identity assurance fails, the sector inherits a compounding risk across every automated service.

Digital identity should be treated as both a platform investment and an emerging threat surface. Post-quantum security planning was raised as an urgent parallel track, given the potential impact of quantum computing on current cryptographic assumptions.

GOVERNANCE SHOULD ENABLE DELIVERY, NOT JUST MANAGE REPUTATION

Participants described a recurring pattern: governance and business case processes that scale poorly for digital work, discouraging cross-agency effort and slowing experimentation. Several noted that governance is often experienced as "tick-box" assurance or risk transfer, rather than an enabler of safe delivery. In contrast, examples were raised where governance was redesigned to support speed, including clearer risk appetite, phased approvals, and mandatory training before access to tools.

If governance is primarily designed to prevent failure, it will also prevent learning. Emerging technologies require structured experimentation, not just compliance.

Redesign governance around two questions: (1) what risk are we accepting and why, and (2) what controls make it safe to proceed, monitor and stop if needed.

MEASUREMENT AND ROI NEED A NEW LOGIC FOR AI-ENABLED WORK

The group challenged traditional enterprise ROI models for AI, arguing much of the value accrues at the individual level (time saved, reduced cognitive load, faster synthesis), and only later aggregates to organisational productivity. Participants observed that pilots often stall because agencies cannot define "day zero" measures, or because they measure the wrong thing: hours saved in a process rather than service outcomes, quality, equity or timeliness.

If success cannot be demonstrated credibly, scaling is hard to justify and risk appetite remains low.

Use mixed measurement: time studies and productivity proxies for internal value, combined with citizen experience indicators (timeliness, accuracy, repeat contact, fairness) for external value.

CHALLENGES AND BARRIERS

PILOT-TO-PRODUCTION FAILURE AND UNCLEAR USE CASES

Participants described AI adoption as dominated by pilots that do not scale. Common causes included unclear problem framing ("using AI because it exists"), lack of baseline measurement, and insufficient attention to workflow redesign. In several cases, automation could quantify time saved, but agencies struggled to evidence improved citizen outcomes.

RISK APPETITE AND CORRECTION CYCLES

Some participants observed that crisis conditions temporarily increased risk tolerance and accelerated deployment, but also created a later "correction mode" where agencies are now fixing rushed decisions. Others cautioned that sustainable adoption cannot rely on crisis-driven shortcuts; it requires trusted, auditable, scalable approaches.

CROSS-AGENCY COLLABORATION FRICTION

A persistent barrier was the transaction cost of working across organisational boundaries: approvals, cost recovery, and unclear incentives. Participants described collaboration as often dependent on executive or political intervention rather than systematic mechanisms. This reduces reuse of proven approaches and increases duplicated effort.

WORKFORCE CAPABILITY AND SKILLS DECAY

Participants raised two workforce risks moving in opposite directions: ageing workforces in specialist domains, and a growing reliance on AI tools that may cause skill decay if not paired with deliberate capability building. This creates both an operational risk (loss of tacit knowledge) and an assurance risk (humans asked to validate uninterpretable outputs.

CITIZEN TRUST AND ASYMMETRY

The group noted that citizens may not distinguish between public and private data practices, and may not understand why government separation of data exists. Without clearer communication, agencies risk being held to high standards without the social licence or buy-in needed to modernise responsibly.

FUTURE FOCUS AREAS

"GOVERNANCE AS AN ACCELERATOR" CAPABILITY SERIES

A practical program on designing governance that enables delivery: lightweight business cases for digital, phased risk approvals, clear decision rights, and integrated auditability. This should include templates that scale down for smaller investments and scale up for high-risk services.

CONTESTABILITY AND ACCOUNTABILITY IN AI-ENABLED SERVICES

A themed roundtable on contestability in the agentic era: what citizens can challenge, how review works, how records are kept, and how reasoning is communicated. Include operational models (review panels, escalation pathways, service standards) rather than principle statements.

IDENTITY, FRAUD AND POST-QUANTUM READINESS

A future session focused on identity integrity, synthetic media threats, and the transition to post-quantum cryptography. Emphasis should be on practical implications: system inventories, upgrade pathways, vendor requirements, and how identity assurance must evolve for high-risk transactions.

MEASURING AI VALUE BEYOND "HOURS SAVED"

A capability workshop on measurement frameworks: baseline design, time studies, service outcome metrics, fairness and error costs, and evaluation methods that reflect citizen experience. Include how to handle the "99.9% good, 0.1% headline" problem through risk-weighted measurement.

WORKFORCE RESILIENCE: AI LITERACY, ROLE REDESIGN AND SKILLS PRESERVATION

Building AI literacy across the workforce, redesigning roles to prevent skill decay, and preserving critical expertise as retirements accelerate. Link capability to governance, so "human in the loop" is a meaningful control, not a symbolic one.

INNOVATIVE IDEAS AND CASE STUDIES

1. MANDATORY TRAINING BEFORE ACCESS TO AI TOOLS

Participants described an approach that treated AI capability like licensing: staff completed mandatory training before being allowed to use approved AI tools. This was framed as a practical trust mechanism, supporting consistent risk understanding, safer use, and a stronger base for audit and assurance. It also created shared language across the organisation, reducing misunderstandings between business, legal, technology and risk functions.

2. DIGITAL AUDIT AND AI READINESS ASSESSMENT AS A SCALING MECHANISM

A notable example described combining policy development, staff training, pilot deployment and an independent AI readiness assessment before rolling out AI enterprise-wide. This was paired with a digital governance framework to balance opportunity and risk, supported by an explicit risk appetite for digital initiatives. The key innovation was sequencing: governance and capability were treated as prerequisites to scale, not compliance after the fact.

3. AGENTIC WORKFLOW REDESIGN IN HEALTH TRIAGE AND BOOKING

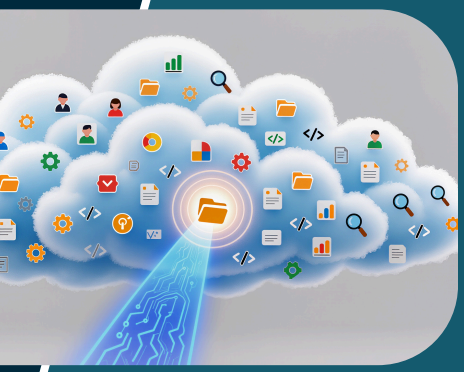
Rather than using AI for clinical decisions, participants highlighted value in automating the operational workload around triage: bookings, preferences, routing and administrative tasks that consume significant clinician time. This reframes AI as a workflow tool that returns capacity to the frontline while keeping decision-making with clinicians. It also reduces risk exposure by applying AI where consequences are less direct, while still delivering measurable productivity gains.

4. INTELLIGENT DOCUMENT PROCESSING TO UNLOCK "DARK DATA"

Industry experience highlighted the ongoing value of intelligent document processing and human-in-the-loop models to extract and structure information embedded in emails, documents and portals. The proposition was simple: much of government's operational data remains trapped in unstructured formats, slowing decisions and increasing manual load. Making data usable at speed was positioned as a direct enabler of better service delivery and auditability.

5. CROSS-SECTOR PARTNERSHIPS TRIGGERED BY FOCUSED PROBLEM SHOWCASES

A practical collaboration pattern emerged: identify a pressing problem, bring in external experts to showcase existing solutions, then formalise multi-year partnerships based on demonstrated alignment with agency needs. The insight was that collaboration accelerates when it is anchored in a specific problem and a credible pathway to implementation, rather than general enthusiasm for innovation.



STRATEGIC OUTCOMES AND RECOMMENDATIONS

IMMEDIATE ACTIONS

- **Establish "day zero" measurement baselines for priority AI use cases**: before new pilots begin, define baseline time, quality and service metrics. Where feasible, use short time studies for individual productivity impacts, and pair them with service indicators such as turnaround time, error rates and repeat contact.
- **Adopt mandatory AI training and usage guardrails**: Implement a minimum training standard before staff access approved tools. Include practical guidance: data handling, limitations of generative outputs, record-keeping expectations, and escalation when outputs appear unreliable.
- **Create a lightweight governance fast lane for low-risk use cases**: introduce a simplified pathway for internal productivity cases (summarisation, knowledge search, drafting, basic workflow automation) with clear control requirements: approved tools, data classification rules, logging and periodic review.
- **Publish clear accountability statements internally**: clarify who owns decisions supported by AI, who reviews AI-generated recommendations, and what records must be retained. This supports both confidence and audit readiness.

MEDIUM-TERM GOALS

- **Redesign business case and assurance templates for digital work**: develop fit-for-purpose templates that reflect iterative delivery, not infrastructure-style certainty. Keep them short, decision-oriented and aligned to risk appetite. Embed options analysis: a non-AI pathway versus an AI-enabled pathway, measured against the same service outcomes.
- **Stand up contestability pathways for AI-supported decisions**: for services where AI informs eligibility, prioritisation or compliance, define how citizens can challenge outcomes, how decisions are reviewed, and what explanation is provided. Build the operational model, not just principle statements.
- **Invest in shared foundations: data products, identity and auditability**: prioritise platform capabilities that multiple agencies can reuse. This includes structured data products, access controls, identity assurance, and monitoring that supports both performance tracking and responsible use.
- **Build workforce capability plans that address retirement risk and skills decay**: identify critical roles at risk, define AI literacy expectations by role, and build pathways for pairing AI adoption with skill development, not substitution.

LONG-TERM VISION

- **Shift from pilot culture to scaled delivery through repeatable patterns**: create a catalogue of reusable patterns for common government needs: triage and routing, document processing, legacy uplift support, audit preparation, and internal case management.
- **Prepare for a post-quantum security transition**: begin inventories of systems reliant on current cryptography, define upgrade pathways, and set vendor requirements for post-quantum readiness. Treat this as a sector-wide resilience program, not an isolated security task.
- **Strengthen social licence through transparent communication**: develop public-facing explanations of how government uses data, what protections exist, and how citizens can exercise agency. Trust will increasingly be a differentiator as digital services become more automated and identity risks rise.

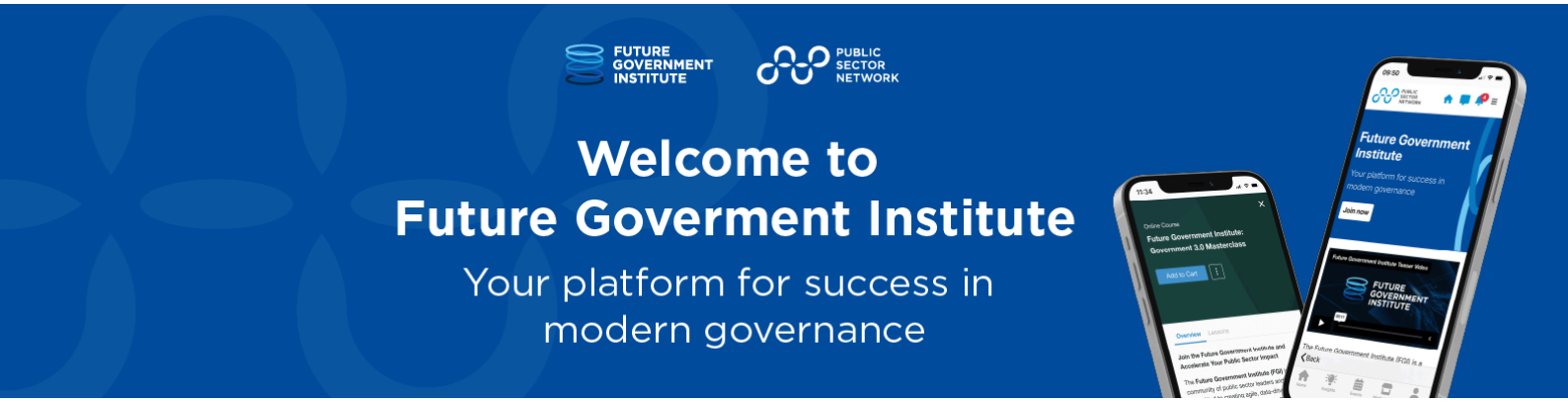
ABOUT THE FUTURE GOVERNMENT INSTITUTE (FGI) RESEARCH COUNCIL

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