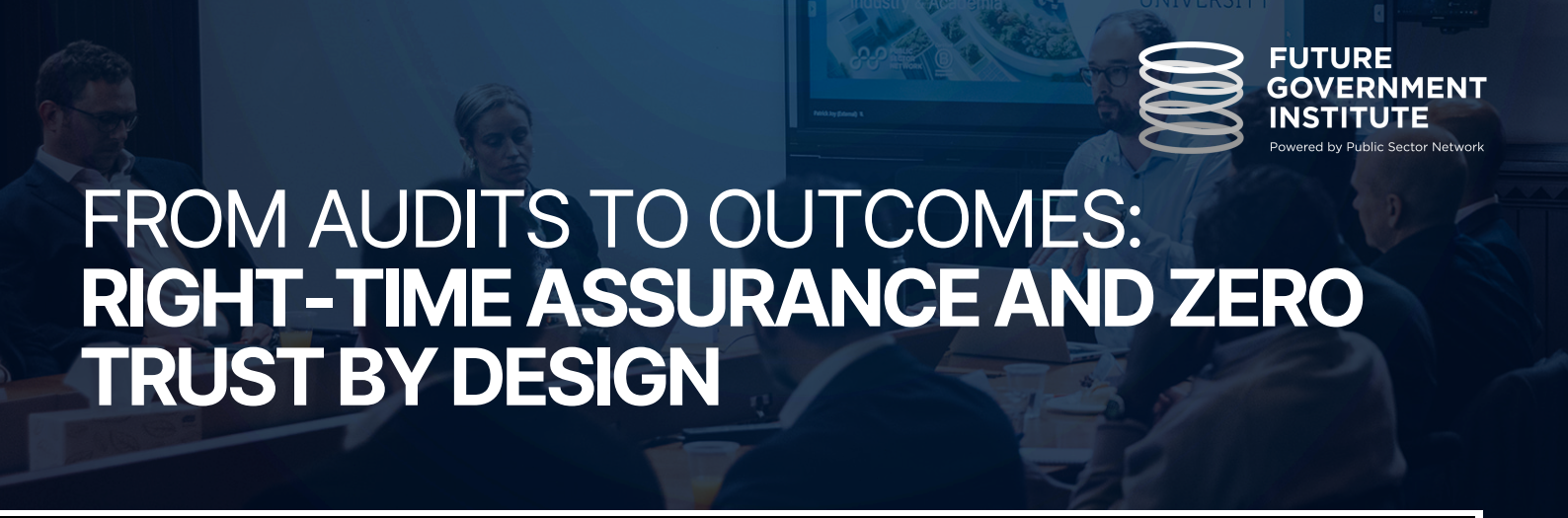


FUTURE GOVERNMENT INSTITUTE
Powered by Public Sector Network

FROM AUDITS TO OUTCOMES: RIGHT-TIME ASSURANCE AND ZERO TRUST BY DESIGN

EXECUTIVE SUMMARY | VOL.30

VICTORIA UNIVERSITY OF WELLINGTON TE HERENGA WAKA

IN BRIEF

Participants described a system that is improving but uneven. Most organisations placed themselves between intermediate and advanced on the cyber resilience journey. The discussion centred on three currents: the economics and timing of certification and accreditation (C&A) activity, the limits of fragmented collaboration, and the need to embed cyber awareness in daily work rather than annual training.

Several agencies reported more than 80 percent of systems certified, yet recurring C&A engagements still cost about $40–50k per solution and are often repeated across government with minimal reuse. Penetration testing delivers clear value, but C&A frequently arrives too late in delivery, leaving legacy risk untreated. Leaders highlighted that trust is a social licence and that visible incident readiness matters as much as prevention.

On collaboration, participants called for practical sharing of artefacts and stories in near real time, not just yearly surveys. Threat intelligence flows reasonably well through national channels, but design patterns, zero trust assessments, and third party risk methods are not being reused enough across agencies of different sizes and risk profiles.

For capability, the group emphasised “desire paths” in user behaviour. People will choose the easiest route to get work done, so secure processes must be the easiest path. Targeted, in-flow nudges, stronger MFA coverage, and routine crisis simulations were seen as high-return moves. The brief concludes with immediate actions to share C&A work, adopt reusable zero trust assessments, stand up a simple cross-agency sharing hub, lift third party risk methods, and widen resilience from cyber only to total organisational continuity.

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

KEY THEMES AND INSIGHTS

"THE CNA MAFIA" AND THE COST OF BEING SAFE

Participants used this phrase to capture frustration with repetitive and expensive certification and accreditation cycles. Value is real when testing finds exploitable issues, but many saw limited return from re-proving the same vendor stack at each agency. A practical shift is to separate reusable product assessments from agency-specific implementation deltas, then share the reusable part. Strategy: create a light shared library of past assessments and penetration test learnings, clearly marked with what is portable and what is agency-specific, and require projects to check the library before engaging a new assessment.

SECURITY THAT ARRIVES ON TIME

C&A often lands after design decisions are locked. That leaves legacy estates untreated and forces retrofit. Several leaders embed security, operations, and architecture under the same objectives so teams do not optimise for speed or safety in isolation. One model used "business advisory groups" that bring product owners, technology, and security together continuously, driving incremental hardening rather than five-year refreshes. Strategy: set entry gates that require risk definition and compensating controls up front, and use zero trust assessments to guide whole-of-organisation posture, not just app-by-app checks.

"DESIRE PATHS" BEAT POLICY

When collaboration tech or data sharing is hard, staff route around it. Email becomes the lowest common denominator. The fix is not more policy. Make the compliant path the easiest path with federated collaboration, approved shared spaces, DLP prompts, and in-flow nudges. Strategy: treat UX as a control. Build rumble strips that warn before a mistake, such as prompts when client numbers appear in mail or when files leave approved locations.

TRUST AS A SOCIAL LICENCE

Leaders linked cyber resilience directly to public trust. Honest self-assessments against protective security requirements lifted capability over time. Incident readiness featured heavily. Teams that practised with crisis playbooks, role clarity, and plain-language communications recovered faster and protected reputation. Strategy: rehearse assume-breach operations and communications, not just patching. Measure time to detect, contain, and restore as core outcomes.

FROM MONOCULTURE TO RESILIENCE BY DESIGN

Recent supply chain shocks showed how a single update can ripple through a technology monoculture. Agencies highlighted third party and concentration risks, including cloud dependencies and open source supply chains. Strategy: diversify where feasible, require software bills of materials, and focus on business continuity outcomes that look the same whether the trigger is a cyber event, a cyclone, or a building outage.

CHALLENGES AND BARRIERS

DUPLICATED ASSURANCE AND LATE CONTROL INSERTION

Repeated C&A work across agencies drives cost without commensurate uplift, particularly when assessments start after architecture is set. Legacy systems remain the long tail.

MARKET NOISE AND "AI SNAKE OIL"

Procurement teams encounter vendors making vague claims around AI features, with limited transparency, explainability, or data sovereignty clarity. The risk of paying enterprise prices for trivial capability is high.

FRAGMENTED INCENTIVES AND THE "UNIQUE SNOWFLAKE" MINDSET

Program pressures often outweigh whole-of-government reuse. Agencies rebuild parallel solutions, then stitch them together later at extra expense.

CAPABILITY SPREAD AND REGIONAL REALITIES

Security expectations are uniform, but capacity is not. Smaller agencies and regional offices face the same threat environment with fewer specialists and less time.

SIGNAL OVERLOAD

Security teams receive a growing volume of vulnerability and incident signals. Triage takes time and attention, and false positives nudge users back to desire paths.

THIRD PARTY AND ECOSYSTEM RISK

End-to-end visibility of suppliers and sub-suppliers remains difficult. Concentration on a few platforms magnifies the blast radius.

FUTURE FOCUS AREAS

REUSABLE ASSURANCE, NOT JUST MORE ASSURANCE

Co-design a two-layer model: shared, reusable assessments for common platforms and products, and a thin agency-specific delta. Pilot it with one widely used service, then scale.

ECOSYSTEM RISK AND CONCENTRATION MAPPING

Run a series on practical third party and concentration risk: SBOMs and model cards, data set bills of materials, cloud dependency maps, and tabletop exercises that cross multiple agencies and suppliers.

AI WITH PROVENANCE

Focus learning on AI assurance that leaders can use: transparency obligations in contracts, evaluation methods, prompt and model risk controls, and secure patterns for agentic workflows.

IN-FLOW LITERACY

Shift from annual modules to in-the-moment cues. Explore lightweight nudges in email, collaboration tools, and data platforms, as well as family-inclusive awareness during national cyber weeks.

TOTAL RESILIENCE

Treat cyber as one hazard in a broader continuity frame. Explore portable connectivity kits, alternate channels, and cross-agency sites that can become regional service hubs during disruption.

INNOVATIVE IDEAS AND CASE STUDIES

1. ZERO TRUST ASSESSMENTS AS A WHOLE-OF-ORG ACCELERATOR

Several agencies reported better value from organisation-level zero trust assessments than from repeated, app-level audits. These assessments surface detection, response, and recovery gaps that apply everywhere. They also help operational teams prioritise identity, network segmentation, and monitoring improvements that reduce blast radius.

2. BUSINESS ADVISORY GROUPS THAT KEEP SYSTEMS EVERGREEN

One organisation convenes product owners, technology, and security as an ongoing advisory group. The group aligns objectives, reduces the yes/no dynamic, and shifts from project cycle spikes to continuous improvement. Security becomes part of routine change, not a late gate.

3. “RUMBLE STRIPS” IN DAILY TOOLS

Instead of relying on memory from last year’s training, teams insert prompts at the point of risk. Examples included DLP pop-ups for sensitive text, safe-share suggestions when external recipients appear, and warnings when files leave approved repositories. The principle is to make the secure choice the easy choice.

4. SECTOR-WIDE SIMULATIONS AND HONEST SELF-RATINGS

Joint crisis simulations across financial regulators strengthened collective response and clarified who communicates what, when. Another agency’s decision to be fully candid in its protective security self-assessment led to a sharp short-term drop in ratings and a sustained uplift over the following years. The lesson is that muscle memory and honest baselines matter more than paper maturity.

5. “STARLINK IN A BAG” AND TOTAL CONTINUITY

Participants advocated for practical continuity kits so offices can stand up core services when networks fail due to cyber or weather events. The same playbooks that pay people in a flood also work during a ransomware outage. This reinforces the shift from narrow cyber thinking to total resilience.

STRATEGIC OUTCOMES AND RECOMMENDATIONS

IMMEDIATE ACTIONS

- **Stand up a simple sharing hub**: Create a lightweight, federated repository for reusable security artefacts: C&A summaries, penetration test lessons, zero trust findings, incident playbooks, and design patterns. Keep it searchable and time-stamped. Start with one or two widely used platforms.
- **Adopt "in-flow" controls**: Expand MFA coverage, turn on DLP prompts in email and file sharing, and enable basic anomaly alerts. Aim for controls that reduce, not add, friction.
- **Rehearse assume-breach**: Run a one-hour tabletop with executive and frontline leaders using existing playbooks. Measure time to decision, clarity of roles, and external communications. Capture gaps and assign owners.
- **Filter the signal**: Configure triage rules so security operations see the few alerts that matter. Use automation where possible to down-rank noisy advisories and raise active exploitation.

MEDIUM-TERM GOALS

- **Reusable C&A with deltas**: Pilot a shared assessment for a common platform. Define what is portable, how to verify currency, and how to document agency-specific deltas. Track cost and time saved across the second and third reuse.
- **Third party risk framework**: Agree a light, common approach that small and large agencies can both use: minimum due diligence set, SBOM and data set bill of materials where applicable, incident notification clauses, and periodic attestations. Align it with existing procurement templates.
- **Zero trust roadmap**: Complete an organisation-level assessment, then fund the top five controls that cut blast radius: strong identity, device trust, segmented networks, centralised logging, and tested recovery.
- **Community of practice that shares in real time**: Extend existing AI and cyber forums into a regular, short cadence session where agencies exchange current stories, not just slide decks. Rotate hosting and keep notes in the hub.

LONG-TERM VISION

- **Total resilience, one playbook**: Merge cyber incident response and business continuity into a single, hazard-agnostic playbook. Ensure communications, welfare, payments, and public information have offline options.
- **Frictionless secure collaboration**: Make the compliant path the easiest path. Federated identity and approved shared spaces should be standard so teams do not default to email for data exchange.
- **Culture that values reuse**: Tie funding gates to evidence of reuse or a clear explanation of why reuse is not viable. Reward teams that publish artefacts others can adopt.

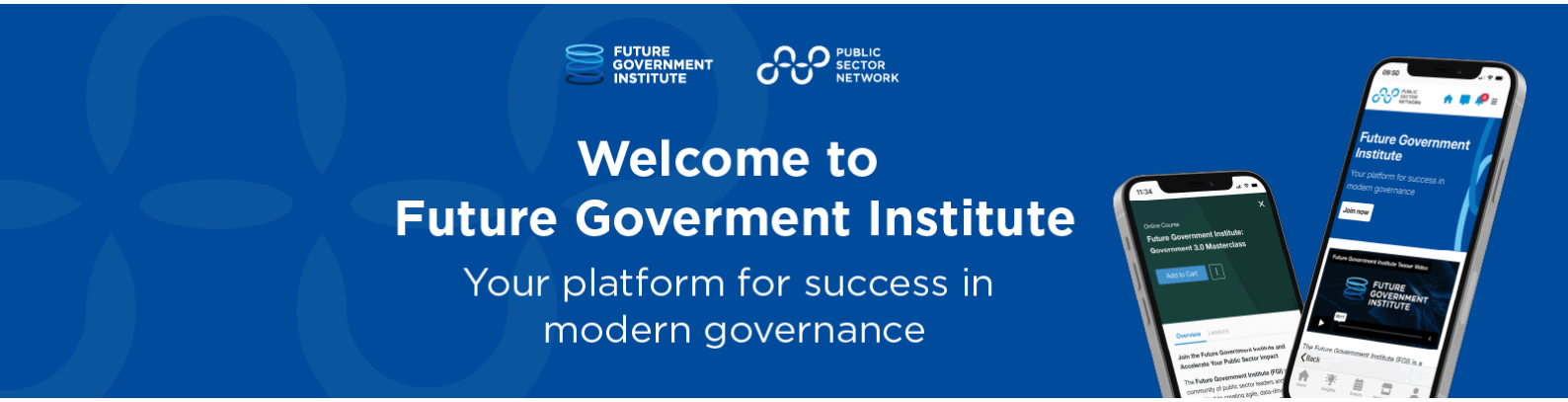
ABOUT THE FUTURE GOVERNMENT INSTITUTE (FGI) RESEARCH COUNCIL

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