CDO TRENDS
Digital & Data Insights for Business Leaders

PURESTORAGE®

WHITE PAPER

The Strategic Pivot: Modernising Federal IT for Trust and Resilience

The transition of government Information and Communications Technology (ICT) echoes the move from private to public utility grids.[1] For decades, agencies built their own costly, bespoke on-site systems demanding specialist skills. The advent of high-speed broadband now allows ICT to be consumed as a utility, paid for by usage. This centralised, 'as-a-service' delivery promises greater efficiencies and improved service delivery, freeing agencies to focus on their core mission.[1],[2]

Three interconnected forces are behind this shift: a digital service mandate[3], a fiscal responsibility imperative, and an evolving threat landscape. Together, they form a causal loop: the digital services mandate demands scalable data; this data is subject to new regulatory compliance; and this, in turn, faces fiscal scrutiny from the Federal CFO.[2]

These concerns make modernising an obligation to fulfil core government functions under new legal and financial frameworks. The table below illustrates how these intersecting forces create a shared mandate for Federal CIOs and CFOs.

Topic	CIO's Strategic Mandate	CFO's Strategic Mandate
Digital Services & AI	Provide scalable, performant architecture to support digital-by-design services. Ensure infrastructure is AI-ready with high-throughput data access.	Steer the transformation agenda for cost control and operational agility. Justify AI and digital investments with a clear ROI.
Cyber Resilience & SOCI Act	Manage technical compliance with ASD's Essential Eight and Protective Security Policy Framework (PSPF). Implement resilient, auditable systems to meet new CIRMP obligations.	Manage financial risks of non-compliance and reputational damage. Ensure investments support government accountability frameworks (ANAO, Senate Estimates).
Procurement & Modernisation	Prioritise platform standardisation and agile, whole-of-government strategies. Reduce operational complexity and technical debt from legacy systems.	Secure predictable OPEX models to avoid costly, high-risk forklift upgrades. Demonstrate value for money and reduce vendor lock-in with transparent pricing.

Hybrid Cloud: The Cloud-Smart Path to Sovereignty and Flexibility

The industry's original "cloud-first" push proved too complex for federal agencies. Australia rightly adopted a "cloud-smart, not cloud-first" approach.[2] The DTA's Secure Cloud Strategy supports this, advocating for pragmatic, risk-based decisions over mandated public cloud migration.[4] For the government, hybrid cloud is the strategic destination — a flexible, resilient operating model aligned with sovereign cloud mandates and data classification protocols, while ensuring the authoritative copy of data remains under agency control.[2]

A solution like Evergreen//One is designed to meet this mandate, providing the flexibility and consumption-based economics of the cloud for your on-premises infrastructure. This approach avoids the financial risk of hyperscaler egress costs and gives agencies control over their cloud service consumption.

The Australian Signals Directorate's (ASD) "Top Secret Cloud" partnership with AWS provides another good example of a targeted, mission-critical use of public cloud for collaboration, not a "lift-and-shift" of all government data.[5] The ASD-AWS approach allows agencies to modernise without losing control, compliance, or continuity.[2]

The role of the data platform

A key challenge for Federal CIOs is the pressure on their virtualisation strategy, particularly due to recent, potentially disruptive, licensing shifts from vendors like VMware.[2] The solution is a flexible data layer that supports multiple transition paths.

This data layer acts as the unifying fabric of the hybrid cloud model, transforming disparate environments into a cohesive ecosystem. Without such a common infrastructure to seamlessly and securely move data across on-premises, public, and private cloud, the DTA's vision of interoperability and shared capability is impossible.[4]

Modernising procurement

Traditional federal procurement, with its long lifecycle and focus on Capital Expenditure (CAPEX), creates budget risk and forces expensive, disruptive "forklift upgrades". Predictable, low-risk procurement is a core priority for government leaders focused on value-for-money.

The Evergreen//One subscription model directly addresses this by providing a predictable Operational Expenditure (OPEX) stream. This model mitigates long-term vendor risk, as agency leaders are increasingly required to demonstrate that they are not locked into a single provider and that they have a practical, real-world exit strategy that can stand up when questioned by procurement or governance bodies.[2] As a unified subscription across on-premises and public cloud environments, it also provides data mobility and flexibility to ensure multi-cloud optionality and a credible exit strategy.[2]

The AI-Data Nexus: From Hype to High-Impact Services

The promise of Artificial Intelligence (AI) to transform government services depends entirely on a clean, secure, high-throughput data platform.[2]

Despite accelerating investment, a 2025 study found that 72% of Australian organisations reported their AI initiatives had under-delivered or were still in early evaluation.[6] The primary causes are a lack of data readiness, unclear Return on Investment (ROI), and significant data gaps.[6]

Accountability and assurance

To succeed, AI requires proximity to trusted data and a new level of accountability. The Digital Transformation Agency (DTA) addresses this with the Technical Standard for Government's Use of Artificial Intelligence (TSGUAI) and the National Framework for the Assurance of Artificial Intelligence in Government. These mandates require AI systems to be transparent, explainable, and trustworthy.[7]

For government AI to be trusted, the underlying data platform must also be intelligent: it needs to "self-optimise" and apply Explainable AI (XAI) to ensure transparent infrastructure decisions.[2] This helps to ground Large Language Model (LLM) outputs in verified data, boosting trust, accuracy, and optimise costs by maximising GPU utility — increasingly a major cost factor.[2]

Enabling citizen-centric services

The success of major citizen services, such as myGov and the national Digital ID program, hinges on a robust, scalable, and trustworthy data platform.[8,9] In this regard, the DTA's effort to build a national data integration infrastructure is essential for connecting datasets and enabling data-driven policy insights.[8]

Without a resilient layer for secure cross-agency data sharing, the vision of a "simple, secure and connected public service" is unattainable. This makes creating the right data platform critical for Federal CIOs, whose mandate is increasingly tied to delivering reliable, accessible services that build public trust.

Strengthening the Digital Shield: The New Reality of the SOCI Act

The most significant and urgent driver for Australian federal IT modernisation is the amended Security of Critical Infrastructure (SOCI) Act. Passed in November 2024, this law fundamentally changed the relationship between government and technology by legally designating "data storage systems that hold business-critical data" as "critical infrastructure assets".[10]

The focus has shifted from physical infrastructure to the data itself as a primary, regulated asset. This introduces non-negotiable legal obligations, directly affecting the CIO's and CFO's risk profiles:

- **Mandatory Incident Reporting:** Entities must report cybersecurity incidents that have a "significant impact" on their asset within 12 hours of becoming aware of the incident.[10]
- **Expanded Government Powers:** The government now has expanded "last resort" powers to direct an entity to take action in response to a "serious incident" that impacts a critical infrastructure asset — not just a cyber incident.[11]
- **Risk Management Program:** The Critical Infrastructure Risk Management Program (CIRMP) now explicitly requires entities to identify and manage risks to their data storage assets.[11]
- **Formal Audit Program:** The Critical Infrastructure Security Centre (CISC) commenced a formal audit program in late 2024, with a 2025 schedule already established.[12]

The legal imperative is clear: choosing a data platform is no longer a technical choice; it is a legal requirement. The IT infrastructure must serve as a "digital shield," governed by mandatory, auditable requirements for resilience and recovery.

Accountability and audit readiness

A core responsibility for Federal CIOs is demonstrating accountability to oversight bodies like the Australian National Audit Office (ANAO) and during Senate Estimates hearings. Recent ANAO audits have highlighted the need for better risk management and oversight of large-scale ICT contracts.[13]

Maintaining alignment with compliance requirements (Essential Eight, PSPF) requires consistent patching and upgrades. With traditional infrastructure, this creates significant operational overhead and

risk. There are solutions: For example, the Evergreen architecture takes lifecycle risk out of the equation by delivering continuous, non-disruptive modernisation. This makes it significantly easier to align with stringent compliance requirements without the usual operational overhead of manual updates and disruptive refreshes, ensuring the infrastructure remains secure and fiscally responsible.

The CFO's Mandate: Predictable Spend, Visible ROI, and Broader Risk Management

The Federal CFO's role now extends beyond finance to enterprise transformation. A major friction point with IT is the lack of cost visibility, particularly in cloud environments, leading to unpredictable, ballooning expenses.6 The traditional model of disruptive, costly "forklift" upgrades is now a financial and operational liability.[2]

Predictable OPEX through subscription

Predictable OPEX models make it easier for agencies to plan, defend spend during ANAO Audits or Senate Estimates, and proactively manage risk. This consumption-based approach eliminates technical debt and avoids stranded assets — a key financial risk when mission priorities or plans change mid-cycle.[2]

A modern subscription model for data infrastructure directly like Evergreen//One solves this by shifting from unpredictable Capital Expenditure (CAPEX) to a stable, predictable Operational Expenditure (OPEX). The result is a low-risk, long-term procurement strategy that aligns with federal budgeting and public accountability frameworks.[14,16]

Mitigating audit and project risk

A CFO's risk portfolio includes financial, operational, and reputational risks from failed projects. The Australian National Audit Office (ANAO) consistently audits major government IT initiatives, frequently recommending stronger governance and risk management to ensure projects deliver on time and on budget.[13]

For instance, an ANAO audit found the Australian Digital Health Agency (ADHA) was "partly effective" in managing a major ICT contract, prompting a risk review. The DTA responded with programs like the Senior Responsible Officer (SRO) to build skills and publishes annual reports to increase transparency.[16,17] This whole-of-government focus on mitigating non-cyber risks is key. A modern data platform's ability to provide an auditable trail and operational stability for these projects is an essential part of the solution.

Conclusion: A Unified Path to a Resilient and Agile Government

IT modernisation is no longer a technical choice; it is a strategic, legal, and fiscal necessity.

The convergence of digital service delivery, AI adoption, fiscal accountability, and evolving cyber threats creates a new, shared mandate for federal CIOs and CFOs. A siloed, reactive approach is now unviable.

The common thread connecting a "cloud-smart" strategy, a trusted AI framework, predictable budgets, and SOCI Act compliance is the data platform. It is the single most critical investment an agency can make to future-proof its operations and meet its mission. A resilient, agile, and cost-predictable data foundation transforms infrastructure from a liability into a strategic asset that secures national interests and builds citizen trust.

Next Steps...

Modernisation is a continuous strategic journey. Agencies must take proactive steps to unify technology, policy, and finance:

- **Conduct an Executive Briefing on Hybrid Data Strategy:** Co-host an executive discussion with technology partners to explore how a modern hybrid data strategy addresses the converging priorities of security, budget, and mission delivery.[2]
- **Map Your Roadmap to Australian Mandates:** Develop an agency-specific roadmap aligned with the Essential Eight and the new SOCI Act amendments. Show how immutable snapshots and data tiering support compliance and reduce fiscal risk.[2]
- **Transform Your Budget with an Evergreen Model:** Explore a consumption-based, subscription model that provides cost predictability and eliminates technical debt. A solution like Evergreen// One gives CFOs confidence to invest in mission-critical IT while providing the flexibility to scale for future digital demands.[2]

References

1 Department of Infrastructure and Regional Development, "National Cloud Computing Strategy," DOCX, 2024

2 Pure Storage, "Modernising Federal IT: Hybrid Cloud, AI, and the Role of Data Platforms," Webinar Briefing.

3 Digital Transformation Agency, "Digital Design to Improve Digital Government Services - Implementation Plan 2024," blog.

4 Digital Watch Observatory, "Australia's Secure Cloud Strategy."

5 Office of National Intelligence, "Top Secret Cloud," news release, July 4, 2024.

6 ADAPT, "How CFOs are driving tech buying and enterprise transformation," 2025.

7 Digital Transformation Agency, "Our next steps for safe, responsible AI in government," blog, September 1, 2024.

8 Digital Transformation Agency, "Digital Design to Improve Digital Government Services," blog, 2024.

9 Digital Transformation Agency, "Data and Digital Government Strategy," website.

10 Critical Infrastructure Security Centre, "SOCI Factsheet - Obligations," PDF, 2024.

11 Lawyers and Partners, "Raising a shield against increased threats to critical infrastructure – SOCI Act amendments take effect," February 2025.

12 PwC, "The Evolution of SOCI," presentation, 2024.

13 Australian National Audit Office, "Audits of Major Projects," 2025.

14 Digital Transformation Agency, "Digital Workforce Data Pilot," report, 2024.

15 Australian Signals Directorate, "ICT and Cyber Skills Shortage," 2024.

16 Digital Transformation Agency, "Major Digital Projects Report," 2025.

17 Australian National Audit Office, "ANAO Report," 2024.

About this White Paper

This white paper was jointly developed with Pure Storage. Information contained in this publication has been obtained from sources and references CDOTrends considers to be reliable, but is not warranted by CDOTrends. This publication may include forecasts, projections, and other predictive statements that represent CDOTrends's and Pure Storage's assumptions and expectations in light of currently available information. These forecasts are based on industry trends, industry expert viewpoints and involve variables and uncertainties. Consequently, CDOTrends makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.