opentext™

WHITE PAPER

Retiring legacy applications and databases: Proven strategies for government agencies

Intermedium

Table of Contents

Retiring legacy applications and databases: Proven strategies for government agencies

This white paper, commissioned by OpenText and developed by Intermedium, addresses the critical need for Australian government agencies to transition from legacy systems to modern, integrated, scalable, and resilient solutions. Despite the clear benefits, many agencies face significant challenges in migrating from outdated applications and databases due to resource constraints, business continuity concerns, and compliance difficulties.

Key points:

1. Challenges of legacy systems:

- Legacy systems pose cybersecurity risks, including system failures and data breaches, due to lack of vendor support and modern security features.
- Non-compliance with evolving privacy, security, and data laws, such as the Australian Privacy Principles (APPs) and Security of Critical Infrastructure Act 2018 (SOCI Act).
- Difficulty in accessing data for decision-making, hindering the use of AI and other modern technologies.
- High maintenance costs and poor employee productivity due to outdated tools.
- Inability to innovate and integrate with new technologies, leading to service failures and high operational costs.

2. Proven strategies for transition:

- **Build an unassailable business case:** Align proposals with government investment drivers to secure funding.
- **Value-for-money assessment:** Compare lifetime benefits to costs to ensure the transition supports agency objectives.
- **Align with Whole of Government (WofG) directives:** Leverage reusable components and resources to increase funding chances.
- **Iterative approach:** Implement smaller, manageable projects to reduce risk and speed up benefits delivery.
- **Focus on data management:** Develop comprehensive data management plans (DMPs) to ensure data quality and compatibility during migration.
- **Modern archiving solutions:** Use contemporary archiving solutions to comply with data management, privacy, and security laws.

Successfully retiring legacy systems involves more than adopting new solutions; it requires strategic planning, robust governance, and alignment with government directives. Contemporary archiving solutions play a crucial role in this process, helping agencies manage compliance and reduce risks. By following the outlined strategies, agencies can effectively transition to modern platforms, enhancing service delivery and operational efficiency.

Definition: Legacy applications and databases

An application or database that requires a transition-off or management plan because it presents an unacceptable risk or negatively affects operations. It has typically reached the end of its lifecycle, lacks vendor support, and is challenging or unfeasible to upgrade.[5]

80%

The typical percentage of an agency's budget dedicated to running systems, including legacy applications and databases—more than in sectors like banking and finance.[6]

Introduction

Every Australian government agency has a digital strategy prioritising the shift from legacy systems to contemporary integrated, scalable and resilient solutions.

> **"By reducing legacy technology, we can more efficiently deliver personalised and seamless services to our communities as well as reduce costs to government."**
>
> NSW Government, NSW Digital Strategy 2024[1]

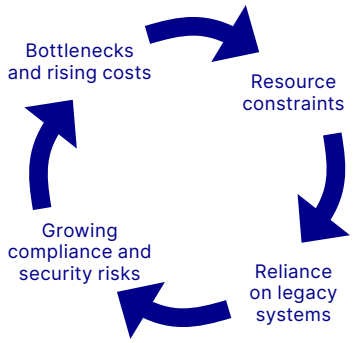
Despite this, many agencies face significant challenges migrating from outdated applications and databases to contemporary solutions, even with awareness of the risks and costs of the status quo.

> **"Government's digital and ICT landscape is characterised by legacy platforms, technical debt, bespoke single-purpose applications, tools approaching end-of-life (and in some cases beyond end-of-life)"**
>
> Digital Transformation Agency, Digital Review 2021[2]

Agencies can be held back for several reasons, including insufficient resources, concerns over business continuity, and difficulties in complying with ever-growing information preservation, privacy and security requirements such as the *Australian Privacy Principles (APPs)*[3] *and Security of Critical Infrastructure Act 2018* (SOCI Act).[4]

These challenges can trap agencies in a vicious cycle of reliance on legacy systems that are difficult to maintain, ineffective, and inefficient.

Agencies can get stuck in a vicious cycle



1 NSW Government, *Digital Strategy,* accessed January 2025
2 Australian Government, *2021 Digital Review*
3 Australian Government, *Australian Privacy Principles,* accessed April 2024
4 Australian Government, *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*
5 See Australian Government, *Managing the Risks of Legacy IT: Executive Guidance,* 2024 and United Kingdom Government, *Commercial and supplier management approach to mitigating and preventing legacy IT,* 2022
6 Australian Government, *Independent Review of the Australian Public Service*, 2019

"Legacy [IT] presents significant and enduring risks to the cyber security posture of Australian Government entities and organisations. Its presence can increase the risk of a cyber security incident, and make any cyber security incident that does occur much more impactful."

Australian Signals Directorate, Managing the Risks of Legacy IT: Practitioner Guidance[10]

The everlasting cybersecurity threat, ballooning maintenance costs, and the inability of legacy applications and databases to meet agency objectives, are prompting leaders to speed up efforts to transition to contemporary platforms. And let's not forget the ever-present need to meet evolving regulatory requirements like the Essential 8[7], APPs and SOCI Act. The question is how to transition successfully.

The NSW Government is adopting a Whole of Government (WofG) approach to support agencies in identifying, monitoring and addressing legacy system risks and challenges through its NSW State of Legacy program.[8] The NSW program offers valuable insights for agencies across Australia.

"NSW is at a turning point in its digital journey, and legacy technology, or outdated digital solutions, can be a challenge in this progress. Government agencies must have the right technology so that they can meet their objectives."

NSW Government, State of Legacy workshop[9]

Leveraging contributions from NSW Government senior executives and a review of publicly available technology strategies, policies and guidance documents, this white paper outlines proven strategies for retiring legacy applications and databases for contemporary platforms.

Legacy applications and databases must go

Risks of keeping the status quo

- **Cybersecurity risks,** including system failure and data breaches. Legacy systems often lack vendor support, the availability of patches and security updates, and modern security features to effectively meet risk mitigation strategies including those in the Essential 8.
- **Non-compliance** with evolving privacy, security and data laws, regulations, standards, and best practices, such as the APPs and SOCI Act. Legacy systems can also hinder an agency's environmental, social and governance (ESG) compliance by lacking the capability to track, report, and manage environmental impact, social responsibility, and governance standards effectively.
- **Difficulty in accessing data and information for decision-making.** Many legacy systems bury valuable insights in cluttered, hard-to-navigate databases. Slow, rigid, and incompatible with modern technologies like AI, they create unnecessary roadblocks for tasks like eDiscovery and responding to freedom of information (FOI) requests. This inefficiency runs counter to agency strategies which emphasise AI as a tool to support smarter, faster decision-making.

7 Australian Government, *Essential Eight,* accessed April 2024
8 See NSW Government, *Insights from the NSW State of Legacy workshop,* 2024
9 ibid
10 Australian Government, *Managing the Risks of Legacy IT: Practitioner Guidance,* 2024

> **"Legacy platforms represent a substantial burden on agencies. Combined with technical debt, they slow delivery and reduce the ability of agencies to adopt innovative technology, integrate with external capabilities, adapt their practices and ways of working, and ensure positive stakeholder experiences."**
>
> Digital Transformation Agency, Digital Review 2021[11]

> **"The longer legacy IT remains in organisations' environments, the harder it will become to find staff with the technical skills to operate and support it. It may also become more embedded in business processes or more difficult to replace as time goes on."**
>
> Australian Signals Directorate, Managing the Risks of Legacy IT: Practitioner Guidance[12]

- **Vendor lock-in.** Agencies are instead trying to develop a diverse supplier ecosystem that champions small to medium enterprises (SMEs) and local providers.
- **Poor employee productivity and frustration.** Government employees expect modern tools that boost productivity, just like those they use in daily life.
- **Inability to innovate** with technology advancements like workflow automation and AI, which requires scalable and high-performing platforms and access to consolidated, high-quality information.
- **Lack of support for agency objectives.** For example, legacy databases may not integrate with contemporary systems, causing information and data silos that prevent the delivery of personalised citizen services.
- **Service failures** that impact citizen outcomes and government trust and reputation.
- **High maintenance costs** from a lack of access to expertise as personnel retire, leave or do not want to work on legacy applications, leading to a reduction in skilled resource availability. This is especially true for cyber security skills where the lack of these resources is a widespread challenge.
- **Inefficient energy usage.** Environmental impact is a growing concern for agencies, especially those that are required to report emissions (e.g. Federal).[13] Legacy systems stand in the way of government environmental goals and long-term taxpayer value by failing to support data minimisation efforts, leading to inefficiencies and unnecessary resource consumption.
- **Complex Machinery of Government (MoG) changes.** Legacy systems can complicate information transfer during a MoG change.
- **Customer disengagement** if legacy systems cannot support rising user experience expectations.
- **Slow speed to value** for agency investments by adding costs and prolonging delivery times.

11 Australian Government, *2021 Digital Review*, 2021
12 Australian Government, *Managing the Risks of Legacy IT: Practitioner Guidance,* 2024
13 Australian Government, *Australian Government Emissions Reporting,* 2024

9%

increase in data breach reports, July-December 2023 to January-June 2024

Office of the Australian Information Commissioner[15]

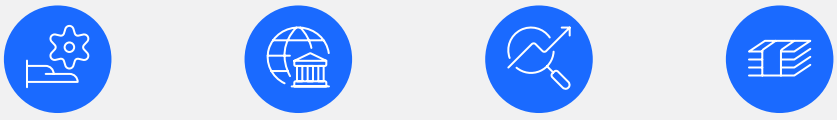
Proven strategies for retiring legacy applications and databases

Build an unassailable business case

Governments are seeking to scale back existing digital and ICT projects and are approving fewer major new initiatives.[14] In this tight budget environment, agencies need to present robust business cases to secure funding.

Agencies can align proposals with one or more of the government's four core investment drivers to increase the likelihood of approval, whether pitching to agency executives or competing in the Cabinet budget process.

Four core government investment drivers



Attending to neglected core services

Reliance on legacy applications and databases can prevent agencies from effectively supporting core services.

One of the key risks in delivering core services is the threat of cyberattacks targeting the extensive data and information managed by government agencies.

Such attacks can compromise citizen privacy, violate the APPs, and may force agencies to take systems offline for containment and damage control. Implementing robust cybersecurity measures, such as the Essential 8 framework, is crucial in mitigating these risks.

Legacy technology can leave agencies vulnerable, relying on outdated architectures and security features that do not effectively provide resilience or support compliance with APPs and Essential 8 requirements.

They can also jeopardise core services that support some of Australia's most vulnerable people.

For example, the recent *Royal Commission (RC) into Defence and Veteran Suicide* found that before the Department of Veterans' Affairs modernised its legacy IT infrastructure under the Veteran Centric Reform program, half of its systems were considered at high risk of failure, with the agency dependent on "niche ICT skills to maintain many of its applications".[16]

14 Cameron Sinclair, Intermedium, *Mid-Year Preview: Debt and Elections Point to Dip in Tech Spending*, 2024
15 Australian Government, *Notifiable data breaches report, January to June 2024*, 2024
16 See Australian Government, *Royal Commission into Defence and Veteran Suicide*, 2024

Managing government finances responsibly

As government debt rises,[17] leaders are under pressure to reduce costs and reallocate resources to maximise benefits to citizens.

Cost optimisation is a key driver for transitioning to contemporary solutions, with reliance on legacy systems often leading to inefficient use of resources.

Although estimating the percentage of agency technology funding spent on legacy applications is difficult, it is thought that legacy modernisation accounts for a major share of investment demand—ranging between 40 and 60 percent.

By retiring legacy systems, resources can be redirected to solutions that improve service delivery or reduce administrative overheads.

Anticipating future needs

Legacy applications and databases can put a drag on data-driven decision-making, which is essential for developing efficient services that meet future demands and requirements.

For example, AI systems are increasingly being used for forecasting, but they require high-quality and consolidated data.

Agencies do not want to be held back as AI opportunities grow. The Australian Bureau of Statistics (ABS) was limited in its participation in the Australian Public Service-wide trial of Microsoft Copilot because HCL Notes (formerly IBM Lotus Notes) held the information and data that would have been subject to the trial and this data could not be accessed by Copilot.[18]

Grow the economy

Agencies need to integrate information and act on evidence-based insights in various areas to support the economy, including grant provision, infrastructure development and regulation. Legacy applications can hinder information sharing and the ability to generate valuable insights.

An unattractive business environment will discourage business investment and reduce the government revenue base.

17 Cameron Sinclair, Intermedium, *Mid-Year Preview: Debt and Elections Point to Dip in Tech Spending,* 2024

18 Eleanor Dickinson, IT News, *ABS parked broader M365 Copilot trial due to 'significant' Lotus Notes legacy,* 2024

Apply the value-for-money test when selecting a legacy retirement strategy

Agencies can conduct a value-for-money assessment to ensure that retiring a legacy application or database supports agency objectives.

The value-for-money test involves determining value by comparing the lifetime benefits (non-financial factors) to the lifetime costs (financial factors).

Value for money = total lifetime benefits - total lifetime costs[19]

While each situation is unique, some typical considerations in a value-for-money assessment may include:

- **Cost reduction:** What are the ongoing maintenance costs of the system versus the migration/retirement costs?
- **Risk reduction:** What are the security, compliance, and operational risks of keeping outdated legacy systems?
- **Business requirement support:** What are the benefits of the replacement system in enhancing operational efficiency, policy development effectiveness and service delivery?
- **Long-term sustainability:** What are the future scalability, support availability, and total cost of ownership?

Options for decommissioning applications and databases— definitions

Replace
Substituting an existing system with a new one that fulfils the same or improved requirements. Replacement often involves transitioning from an on-premises application to a cloud-based service.

Refactor ("modernise the code")
The process of restructuring existing code and architecture to make it more efficient and maintainable, without changing its core functionality. Refactoring often involves migrating monolithic applications to a microservices architecture, which is the preferred approach of most WofG architectures. Agencies can leverage AI to support and accelerate refactoring code.

Re-platform ("lift and tweak")
Migrating an application to new infrastructure while taking advantage of new functionalities, e.g. access to microservices via APIs.

Re-host ("lift and shift")
Moving an application from one environment to another without changes to the code or architecture (e.g. from an on-premises data centre to the cloud). This approach may allow access to the benefits of new infrastructure (e.g. cost or stability) without changing an application's functionality.

19 NSW Government, *Value for money,* accessed February 2024

Agencies may also choose to “retire” a system without transitioning to an alternative, for example when a program relying on an application is completed.

Migration strategies meeting selected value for money test considerations			
Approach	**Reduce costs**	**Reduce risks by improving security**	**Support business requirements**
Replace	✓	✓	✓
Refactor (modernise code)	⚖	✓	✓
Re-platform (“lift & tweak”)	⚖	⚖	⚖
Rehost (“lift & shift”)	⚖	⚖	✗

⚖ Maybe

Align with Whole of Government directives

“Reuse before Rent before Buy before Build”

Victorian Government, Digital Technology Guidelines[20]

Agencies are more successful in decommissioning legacy systems when their strategies align with WofG directives. This alignment allows them to leverage reusable components and resources, including support from the WofG digital agency. It also increases their chances of accessing funding through WofG ICT and digital funding pools.

Four jurisdictions (NSW, Western Australia, Tasmania, and South Australia) have dedicated budget mechanisms to encourage ICT and digital projects that support WofG priorities. These mechanisms, with their funding pools, can reject submissions that do not align with government objectives.

All Australian jurisdictions now have a WofG ICT architecture. Although expressed differently across jurisdictions, these typically require agencies to share already-established components, go cloud-first and focus on interoperability and simplicity.

20 Victorian Government, *Digital technology guidelines*, accessed February 2024

WofG architectures dictate the following attributes:

- Modular
- Cloud-first
- Simple modern user experiences
- Digital by default
- Responsive
- Configuration over customisation
- Reusable components
- Compliance with privacy and security requirements, including the Essential 8 and APPs

"The Australian Government commits to ensuring technology is scalable, secure, resilient and interoperable, with new systems and infrastructure that supports data access and discoverability."

Australian Government, Data and Digital Government Strategy, 2023[21]

Digital government leaders, such as NSW, maintain platform solution libraries for use by multiple agencies. NSW's State Digital Assets (SDA) is a directory of platforms, services and data, including for digital licencing and permits, payments, spatial data and grants management.

CASE STUDY: NSW Government tackling legacy using collaboration

The NSW Government is taking on challenges associated with legacy systems through a collaborative, WofG initiative led by Digital NSW within the Department of Customer Service (DCS).

Digital NSW is one of the most active digital/ICT oversight agencies in Australia, which has led to the NSW Government becoming Australia's digital government leader.[22]

Central to this initiative is the State of Legacy report, developed following extensive consultation with NSW agencies and industry experts. The report contains several recommendations to support agencies in reducing risk and legacy accumulation, including:

Establishing the foundations for legacy reform

- Standardise legacy definitions and data capture to identify and measure the scale and impact of legacy systems on the environment, economy and society.

Prioritising and facilitating benefits management

- Support a consistent approach to prioritisation.
- Establish a baseline to measure the effectiveness of investments and to guide reform.

Investing to mitigate high-risk legacy harms

- Improve return on investment and success in system modernisation through standards, governance and assurance.
- Prioritise funding for systems with the highest risk of impacting communities, the economy, or the environment.

21 Australian Government, *Data and Digital Government Strategy*, 2024
22 Intermedium, *Digital Government Readiness and Maturity Indicator,* 2024

Proactively reducing legacy technology accumulation

- Reduce the cost and impacts of legacy, through consolidation, standardisation, and reuse.
- Retain and build skills in legacy and emerging technologies, reducing risk and cost.

Digital NSW is using the recommendations to develop a phased approach to achieving outcomes.

The NSW Government is also piloting a legacy risk framework with risk parameters including supportability, security and potential impacts on the community, economy, and environment.

The assessment establishes a baseline with average risk levels, estimated timeframes for modernisation and an inventory of systems that serves as an indexed tracker to monitor legacy technologies.

Take an iterative approach to modernisation

Australian governments have no appetite for “big bang” projects.

Instead, governments prefer smaller and more manageable projects to reduce risk and speed up the delivery of benefits.

In the past, initiatives to retire legacy systems were often accompanied by cost overruns, as unforeseen migration challenges and insufficient planning led projects to exceed schedules and budgets.

A further reason for the change is a renewed focus on SMEs and local suppliers. Focusing on iterative progress creates opportunities for smaller businesses to participate as they may not have the scale of larger suppliers, with agencies deeming them “too risky” for high-value projects.

The iterative approach can also minimise disruption to user experience, as new features are introduced incrementally. This can help in organisational cultures that resist change by taking internal personnel along the journey.

CASE STUDY
Services Australia review recommends iterative projects

In late 2024, former Telstra CEO David Thodey completed a Capability Review of Services Australia, revealing a heavy reliance on legacy systems.[23]

He found that these systems, while functional, hinder efficient service delivery and integration of emerging technologies and that their maintenance depends on employees nearing retirement.

An internal survey as part of the review highlighted that 62 percent of respondents identified ICT as a critical area for improvement.

The review found that an iterative approach to transformation would support agency objectives.

"While some re-platforming may still be required, significant architectural improvements can be achieved progressively, continually delivering new functionality to the agency."

"This would present the agency with an opportunity to run its legacy systems in parallel with other technologies, iterating over the short-term to ensure it maintains agility to keep pace with emerging technology."

In response, Services Australia has initiated new efforts to modernise its technology infrastructure, including the development of a 10-year ICT Architecture Strategy and Plan, expected by June 2025.[24]

Focus on getting agency information in order

A key challenge when retiring legacy systems and transitioning to modern platforms is that inadequate data standardisation, compatibility, and quality, which can lead to integration difficulties, increased migration costs, and potential disruptions in business operations. This is particularly challenging when data and information are spread out across multiple generations of technology. Therefore, extensive planning is vital before retiring legacy systems, with consideration given to clearly defining the purpose of the initiative and addressing data and information challenges.

Data management plans (DMPs) are a best practice approach to ensuring that agency data and information are well-managed across their lifecycle and that adequate systems support agency objectives.[25] DMPs include a statement of the agency's objectives for collecting, creating or storing data or information and how this will support an activity, project or business area.[26]

23 Australian Government, *Capability Review Services Australia,* 2024
24 Eleanor Dickinson, IT News, *Services Australia draws up 10-year IT architecture strategy,* 2025
25 Australian Government, *Data governance and management,* accessed January 2025
26 DMP best practices have been informed by the Australian Government, *National Archives of Australia's Data management plan template*

The agency's DMP should include project start and end points, collection and update schedules, timeline reviews, retention periods and information and data relationships. Other additions may include maps of data flows in business processes to understand the costs of storing and moving data.[27]

Agencies can align their DMPs with their technology modernisation roadmaps, which include decommissioning timelines, stakeholder responsibilities and assurance functions.

When developing or updating the DMP, agencies may find they are retaining information that can be disposed of because there is no reason to hold onto it. Once a retirement project has commenced, agencies will need to rely on DMPs and information registers to ensure that data and information are synchronised correctly between legacy and contemporary systems.

Effective synchronisation requires various tools and processes, including data migration software, regular audits, and validation checks to maintain accuracy and prevent discrepancies. Information mapping is needed to ensure compatibility between different technologies, and version control and backups safeguard against loss.

Contemporary solutions provide high levels of automation for all these processes, including data extraction, transformation, and loading, reducing demand on personnel.

27 Identified from Intermedium's questionnaire to Department of Customer Service, 2025

Use modern archiving solutions for compliance

Reliance on legacy applications and databases may prohibit agencies from complying with new data management, privacy and security laws, regulations and policies.

A critical step in ensuring compliance when transitioning from legacy systems to contemporary platforms is establishing a fit-for-purpose archive.

Modernising for data retention and records preservation

Government data and records policies require that information be migrated during technology changes in a way that keeps essential characteristics unchanged,[28] including preserving context.

Agencies may struggle to comply with this requirement if data and information sit within various systems; for example, procurement information may sit in both an ERP system and a separate contract management system.

Agencies can deploy contemporary archiving solutions to integrate information from diverse sources. These solutions allow:

- Agencies to standardise, cleanse, and reshape data before loading it into the new system.
- Information to be preserved in context.
- Users to ensure that compliance procedures are applied.

Contemporary archiving solutions support structured and unstructured information along with the various formats used by agencies.

These solutions can analyse, classify, and protect structured and unstructured information throughout the information lifecycle, automating the security, retention, and preservation aspects of the archive.

Modernising for ease of information access

Agencies require archiving that allows information and data to be easily accessible for business requirements, for example, to support research and reporting or comply with freedom of information (FOI) requests.

Government information is often stored in different systems and formats (structured, unstructured, semi-structured) making the development of a joined-up view difficult. Furthermore, agencies often insufficiently catalogue systems and data, meaning employees do not know where to look for the information they need.

Contemporary archiving solutions offer advanced search functionality that allows for easy access to records or data points, supporting users to conduct audits or retrieve information without requiring the upkeep of a legacy database.

28 For example, see NSW Government, *Digital Records Preservation Policy*, accessed January 2025

Modern REST APIs streamline information access by enabling secure, real-time data sharing across systems, breaking down silos and improving efficiency.

These solutions also allow for the export of reports in various formats, for example, raw data or PDF files, while keeping track of the relationships between information and sources.

User-friendly product interfaces lower the learning curve for employees and reduce resistance to change.

Modernising for information privacy and security

Government systems often contain sensitive information and data that must be handled in compliance with laws and regulations, such as the *Privacy Act 1988,* which are accompanied by heavy penalties.

Therefore, security is a foremost concern when retiring systems and archiving information.

Agencies can safeguard information and data using solutions that offer:

- **End-to-end encryption** of sensitive data at rest and in transit. Contemporary solutions help agencies pinpoint which data needs encryption, avoiding unnecessary encryption that wastes capacity, drives up costs, and increases emissions via unneeded infrastructure.
- **Advanced access controls** so only authorised personnel can access or modify sensitive data.
- **Logging and auditing** supporting traceability.
- **Data masking** to anonymise sensitive data including personally identifiable information (PII)

Contemporary archiving solutions provide high levels of security and ensure that information remains accessible to authorised personnel and auditable throughout the retention period, as well as “defensible deletion,” which means that information disposal is proactively and methodically managed according to information governance requirements.

Archiving solutions that integrate information governance processes also help agencies reduce the accumulation of redundant, obsolete and trivial (ROT) data. Eliminating this excess data lowers costs, reduces emissions and minimises the risk of cyberattacks by shrinking the attack surface.

These solutions also allow authorised personnel to scan for sensitive data and PII to ensure that risk-appropriate controls are in place.

Archiving: Vital for compliance		
Compliance requirement	**Status quo challenge**	**An archiving solution should:**
Data retention and records preservation e.g. NSW Digital Records Preservation Policy	• Information in multiple systems and formats • Information must migrate with tech changes keeping characteristics	• Integrate diverse information sources • Automate information governance • Preserve the original context of the information • Enable scalability • Support structured and unstructured information
Information accessibility e.g. Freedom of Information Act 1982	• Information in multiple systems and formats • No “joined up view”	• Support advanced search • Enable export in various formats
Information privacy and security e.g. Australian Government Information Security Manual	• Everlasting cyberthreat • Digitisation is rapidly creating more information	• Support data masking and PII identification • Support access control and auditing

Focus on project governance and benefits realisation

Project and portfolio management is not just for personnel implementing new applications and solutions. The same rigour must be applied to decommissioning legacy systems, with each step mapped back to the expected cost- or risk-benefit to ensure value for money.

Establishing effective governance is crucial as legacy retirement projects often encounter a variety of challenges, including insufficient documentation, difficult integrations, and complicated middleware implementations.[29]

By having clear objectives and continuously aligning efforts to achieve them, agencies can prevent scope creep and ensure that the project delivers the expected benefits. Personnel must also secure support from senior leadership by clearly articulating the strategic value and anticipated benefits of the transition. Developing this support from the project’s outset is critical to maintain momentum.

Additionally, outdated security architectures risk exposing sensitive information during migrations, necessitating meticulous planning and security controls including access controls, encryption and continuous monitoring to detect and mitigate potential threats.

29 Identified from Intermedium’s questionnaire to Department of Customer Service, 2025

Adhering to established project management best practices, such as using common standards and effective communication, also enhances the likelihood of a successful legacy project.

Next steps

While the above strategies are key to maximising an agency's success, there are simple yet impactful first steps agencies can take to fast-track their journey. They include:

Creating/updating the agency legacy system modernisation strategy

- Register existing systems and dependencies
- Map business capabilities to systems (not vice versa)
- Prioritise modernisation using value-for-money assessments

Creating/updating information and data management plans

- Information and data management plans help ensure that data and information are effectively managed across their lifecycle with systems that support agency objectives.
- Align the plans with the legacy system modernisation strategy.

Securing stakeholder buy-in

- Align efforts with agency and WofG objectives to build support from decision-makers and funding bodies.
- Collaborate with the WofG digital/ICT coordination agency.

Leveraging industry expertise

- Find partners with proven experience in decommissioning and modernisation.

Conclusion

This white paper outlines proven strategies for agencies transitioning from legacy applications and databases to modern platforms effectively. Key strategies include developing an unassailable business case to secure support, applying value-for-money assessments when selecting approaches, and aligning initiatives with WofG directives.

The paper also emphasises the importance of taking an iterative approach, instituting strong project governance, and focusing on benefits realisation.

While successfully retiring legacy systems and transitioning to modern platforms involves much more than just adopting new solutions, having the right enabling technologies is critical. The paper outlined how contemporary archiving solutions play an essential role in the process, supporting agencies to reduce risk and manage compliance with information preservation, accessibility, privacy and security requirements.

Resources

Learn more ›

About Intermedium

Intermedium researches the Australian and New Zealand public sector's use of information and communication technology and progress in digitising government services. Our independent and objective analysts utilise qualitative and quantitative data to analyse public sector trends in technology adoption, funding levels, and procurement. Almost 100 public and private sector clients utilise our syndicated content and online dashboards, consulting and research services.

About OpenText

OpenText solutions empower public sector organisations to optimise workflows, enhance citizen services, and ensure compliance with regulatory standards. By leveraging advanced content management, data analytics, and secure collaboration tools, OpenText transforms information chaos into actionable insights that power government efficiency and collaboration. OpenText innovations provide frictionless citizen experiences and streamline mission-critical processes, all while providing bank-grade cybersecurity. OpenText is trusted by the Top 20 national governments around the world to address critical IT needs and public sector mandates under a single umbrella. With more than 35 years of trusted partnerships across the public sector, OpenText is at the forefront of enabling AI-driven breakthroughs. Learn more at: opentext.com/solutions/industry/public-sector.

OpenText is the leading information management software and services company in the world. We help organisations solve complex global problems with a comprehensive suite of business clouds, business AI, and business technology. For more information about OpenText (NASDAQ/TSX: OTEX), please visit opentext.com.

opentext™