Publication date:
26 June 2020
Author:
Tony Castley

Accelerating Digital Transformation in Government with the Right Technology Approach

How Micro Focus can support digital transformation in federal government agencies

In partnership with:

Brought to you by Informa Tech

Contents

Summary

Constituent and market demands are compelling Australian federal government institutions to realign their functions and services. The foundation of this citizen-centricity is a holistic and personalised view of each person's life journey derived from the data held by government agencies. The Digital Transformation Agency is responsible for driving change across the Australian public sector through initiatives such as the Digital Transformation Strategy. In parallel, the national data commissioner is preparing the new Data Availability and Transparency legislation to free data from its current silos and make it available for these new citizen-centric services.

Significant challenges exist that impede a government agency's ability to deliver against the Digital Transformation Strategy. Omdia and Micro Focus have partnered on a survey of 40 Australian federal government decision-makers to gauge the maturity of and progress on agencies' digital transformation initiatives and the underlying technology challenges and investment. The survey and follow-up interviews covered each agency's digital transformation progress and maturity, data and analytics capabilities, use of artificial intelligence (AI) and intelligent automation, implementation of DevSecOps practices, and future technology investment plans.

Study findings

A quarter of all respondents stated their agency did not have an approved digital transformation strategy. Larger agencies and departments were more likely to have a mature digital transformation programme with executive support and funding. Most respondents were aware of their relative progress and maturity.

Respondents understood that the proposed Data Availability and Transparency legislation would have a significant impact with 88% of the respondents stating that IT systems would have to change and a substantial 45% saying that new systems or major changes to existing systems would be required. Just over half believed it would have a significant impact on their agency's data governance practices.

These statistics show that many federal government agencies have a lot of work to do on their strategic direction and core data governance and management activities.

With the extensive use and capability of AI, it is surprising to note that 38% of respondents stated that their agency had no plans to implement AI. Where the investment is happening, it has historically focused on internal problem spaces; however, respondents indicated that future expenditure would focus on citizen services including case management, citizen identity, and citizen self-service.

Agencies are embracing intelligent automation technology with 84% having current or planned implementations, mainly targeted at internal improvements to the back-office process, data usage, and data quality.

Government agencies have a long way to go in the adoption of DevSecOps, with only 7.5% scoring top maturity marks for the best teams. Work is starting on organisational

structures, but significant challenges exist around legacy technology and the adoption of DevSecOps tools to automate and accelerate the practice. The survey and interviews indicate that many agencies are using the title *DevSecOps* without implementing the key principles, practices, and technology that it implies. These results may also reflect an underlying misunderstanding of the DevSecOps practice and scope.

Recommendations

Successfully transforming federal government agencies into citizen-centric data-driven digitally enabled organisations requires significant work. It needs not just a more strategic use of data and analytics but new operating models and tools for engagement with constituents.

Digital transformation in government requires the strategic use of existing and emerging technologies and practices. With limited resources, agency CIOs need to leverage AI and intelligent automation to release resources and deliver meaningful transformation without breaking the bank. The nature of the data holdings and services provided by the federal government requires security, compliance, and risk to be considered across all aspects of a capability. For CIOs, DevSecOps principles place security at all points of technology acquisition, development, and operations, ensuring the ongoing integrity of data holdings.

Applying the right tools with the right culture can deliver benefits that accelerate the delivery of real business value much faster than expected by

- Enabling high-quality data as the foundation for digital delivery
- Leveraging this new high-quality data to drive insight through analytics and AI
- Integrating those insights directly into critical business decision-making processes
- Consistently applying security, risk management, and governance across the organisation
- Freeing resources from repetitive work so they can concentrate on transformation

Applying useful data, analytics, AI, and intelligent automation will allow policy areas to focus on stakeholder engagement and allow service delivery areas to put the human touch into the service by understanding the background and situation of the person receiving the service. These changes do require the consideration of delegation within the service and a serious conversation about employee responsibilities to ensure staff can perform these higher functions.

Leveraging technologies – such as those provided by Micro Focus – allows organisations to extract value from existing investments while increasing agility and responsiveness to change. Investment in IT management tools that can span and bridge most of an agency's technology portfolio and are underpinned by a consolidated security layer will ensure an agency can meet its strategic digital transformation goals without compromising security or trust.

Current state of digital transformation in the Australian federal government

Elements of a good strategy

Enacting a digital transformation strategy requires the inclusion of some key aspects covering technology, operating model, organisational structure, culture, and budgeting.

Omdia's research looked beyond the obvious to see whether the agencies covered culture and process in their strategies and are actively providing executive and financial support for transformation. Table 1 shows the aspects of the survey used to expose the relative maturity and completeness of the agency's digital transformation strategy.

Table 1: Indicators of digital strategy maturity

	Least mature	Most mature
Strategy document	Under development	Approved and implementing
Executive responsible for strategy outcomes	IT executive	Dedicated executive (e.g., CDO)
Scope of change	No organisational change	Organisational change across whole agency
Linked to HR capability planning	No link to HR plan	Linked to HR plan
Funding programme	No dedicated agency funding	Dedicated agency funding

Source: Omdia

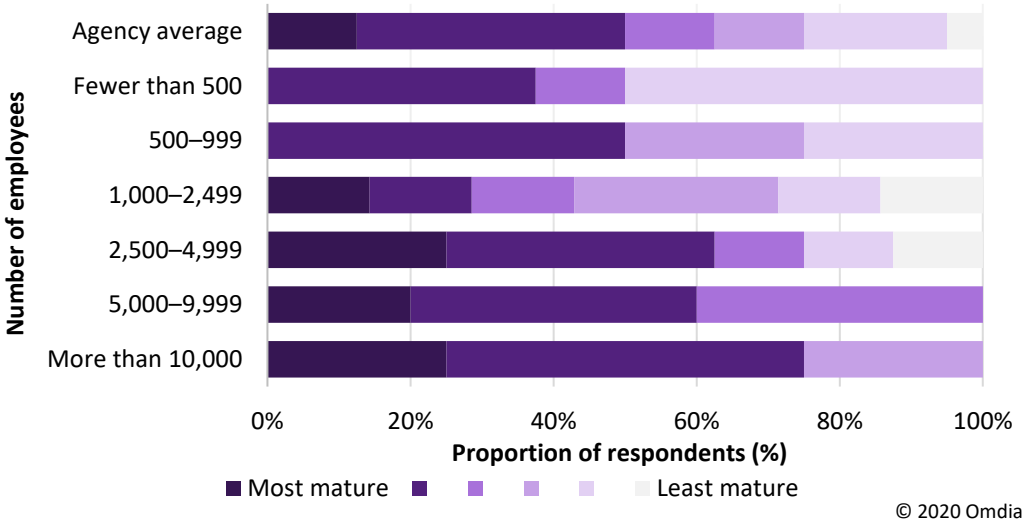
Respondents that stated their strategy was still under development or in draft were considered to have the lowest two levels of maturity regardless of their other responses. The strategy needed to be at least approved before other factors were considered. The data did show some agencies had progressed with organisational changes and funding to drive the development of a formal strategy.

Survey results

Our survey results show that Australian federal government agencies have been hard at work on their digital transformations. Eighty per cent of respondents said that their strategies are approved, 68% said funding has been made available, and 90% said that there are supporting organisational changes to implement the strategy.

The results of the survey (Figure 1) show a significant divergence across agencies, with only 12.5% of all respondents ranking full maturity marks and 25% with strategies not yet approved. Half of all respondents work in agencies with a well-advanced and comprehensive digital transformation programme underway (top two rankings). A general trend is evident that aligns maturity to the agency's size. Smaller agencies with fewer than 1,000 employees struggle to meet the requirements of the highest maturity level. Few can afford to establish an executive position solely dedicated to running the transformation programme, and some are progressing without specifically allocated funding, instead using the strategy to inform individual investment decisions.

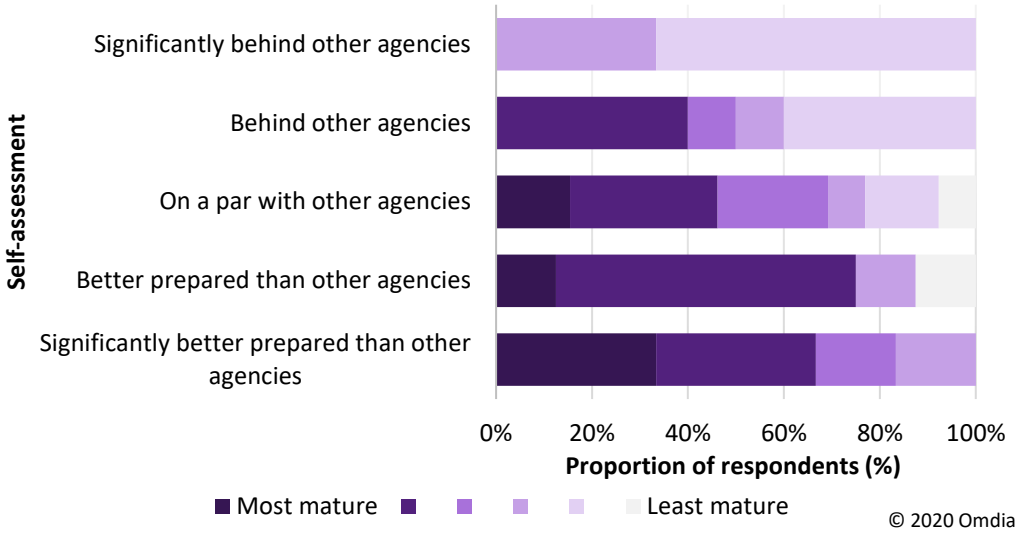
Figure 1: Digital strategy maturity by agency size



Source: Omdia

When respondents were asked how they ranked their agency against others, there was a high correlation with our maturity assessment (Figure 2) with few outliers. This general awareness of the other agencies' progress has increased with the introduction of the COO and CIO forums.

Figure 2: Digital strategy maturity against self-assessment



Source: Omdia

Follow-up interviews exposed differences in the importance placed on digital transformation across agencies. As might be expected, agencies with a heavy policy or administrative focus placed less weight on the importance of transformation than those with direct constituent services.

Omdia view

Over the last few years, the Australian federal government has provided guidance and applied pressure on agencies to progress their digital transformation. Through the Digital Transformation Agency (DTA), a more strategic and top-down approach has been added to the previous bottom-up agile software-delivery focus that prevailed before. The government Digital Transformation and Secure Cloud strategies have provided a framework for agencies to progress along their own path without feeling as if they are breaking new ground.

Agencies have responded, and according to our research, 50% are implementing transformation programmes now. They are taking a broad view with an understanding of the impact on their budget, skills, operating models, and organisational structures. Smaller agencies are less advanced, because they struggle to transform and continue to operate within their resource limits.

Digital transformation requires quality data and scalable analytics

The end state of a digital transformation programme is an agile organisation that employs digital technology to understand the consumer and continually improve and manage its business. This understanding comes from data collected and utilised by the organisation and the insights derived from it.

Government agencies have increasing stores of data, collected and maintained at significant cost. This data, collected in the course of delivering government services and policy development, has historically been stored separately from other data and used only for the "purpose for which it was collected". This transaction-centric data, kept for compliance reasons, is an expense to agencies, especially when much of it is kept in the original system, incurring software licence and infrastructure costs. However, the same data opened for appropriate, managed use is an asset that will enable agencies to provide citizens with a more seamless experience, reduce waste, and deliver significant social outcomes.

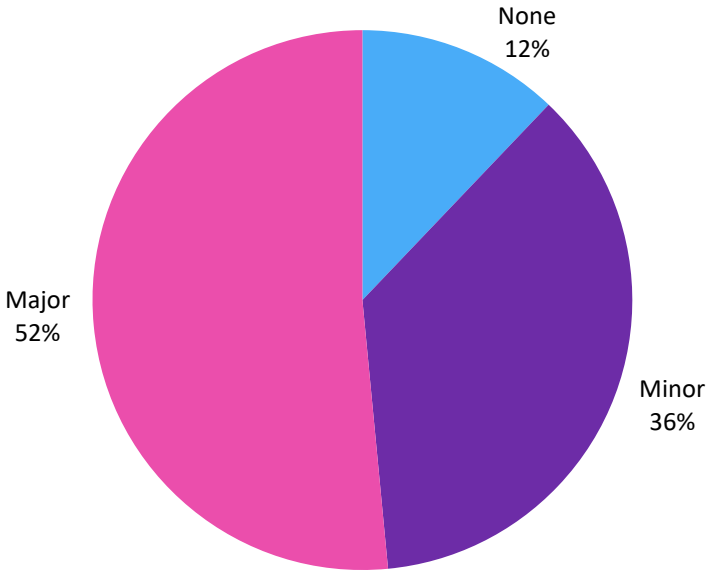
A survey undertaken by the Australian National University shows that over 90% agreed that the government should use data to target services and resources. The same survey showed that 45% disagreed with the statement that "government is open and honest about how data is collected, used, and shared". So government has the social licence to use the data it obtains to deliver services but needs to be more transparent around its use to retain trust.

Data Availability and Transparency legislation

New policies and legislation are required to give a framework for government decision-making on individual data sets. In Australia, this is being addressed by the national data commissioner with the proposed Data Availability and Transparency legislation (previously titled Data Sharing and Release). This legislation will provide authorisation to government agencies to share government data with accredited users, including other government agencies at all levels and non-government entities such as universities. Under the proposed regime, if current legislation does not permit the sharing or release of data, government agencies will have a mechanism to test whether the purpose is valid and whether appropriate controls can be applied to ensure data privacy is maintained. The same legislation empowers the data commissioner to develop requirements and guidelines to support all stakeholders.

The vast majority, 83%, of our survey respondents were aware of the legislation, and 52% believed it would have a major impact on their agency's data governance practices (Figure 3).

Figure 3: Data availability legislation's impact on data governance practices



Source: Omdia

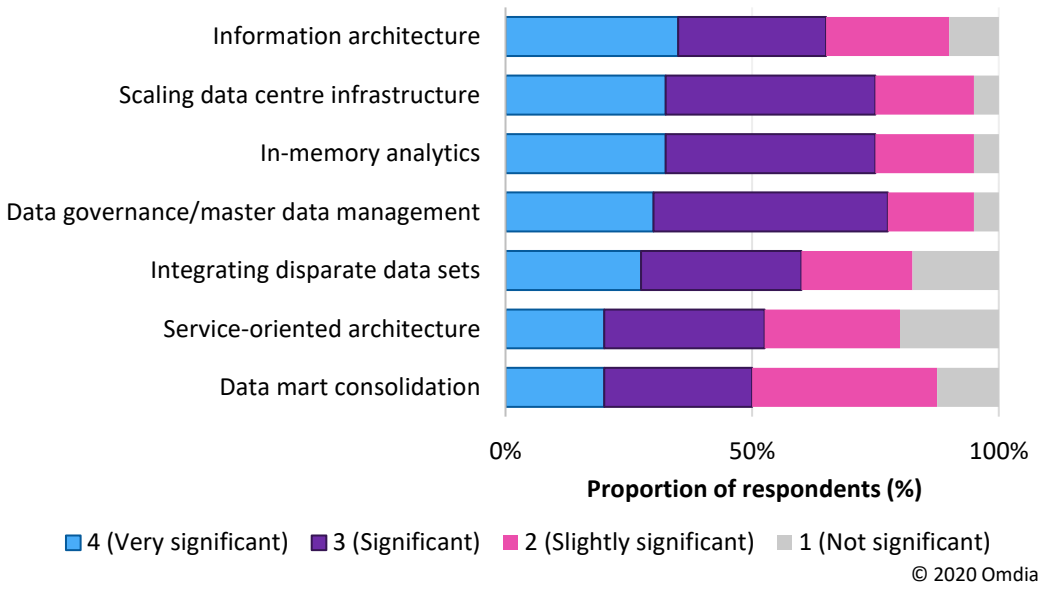
Eighty-eight per cent of respondents also stated that IT systems would have to change to support the new legislation, with a substantial 45% stating that new systems or major changes to existing systems would be required.

Data and analytics challenges within agencies

External drivers such as the new legislation are exposing significant challenges in leveraging data and analytics within their agency. These challenges, identified by our respondents, shed light on the process and technology changes alluded to above.

From a big data viewpoint, agencies have highlighted significant challenges around information architecture, data governance, and scaling technology (Figure 4).

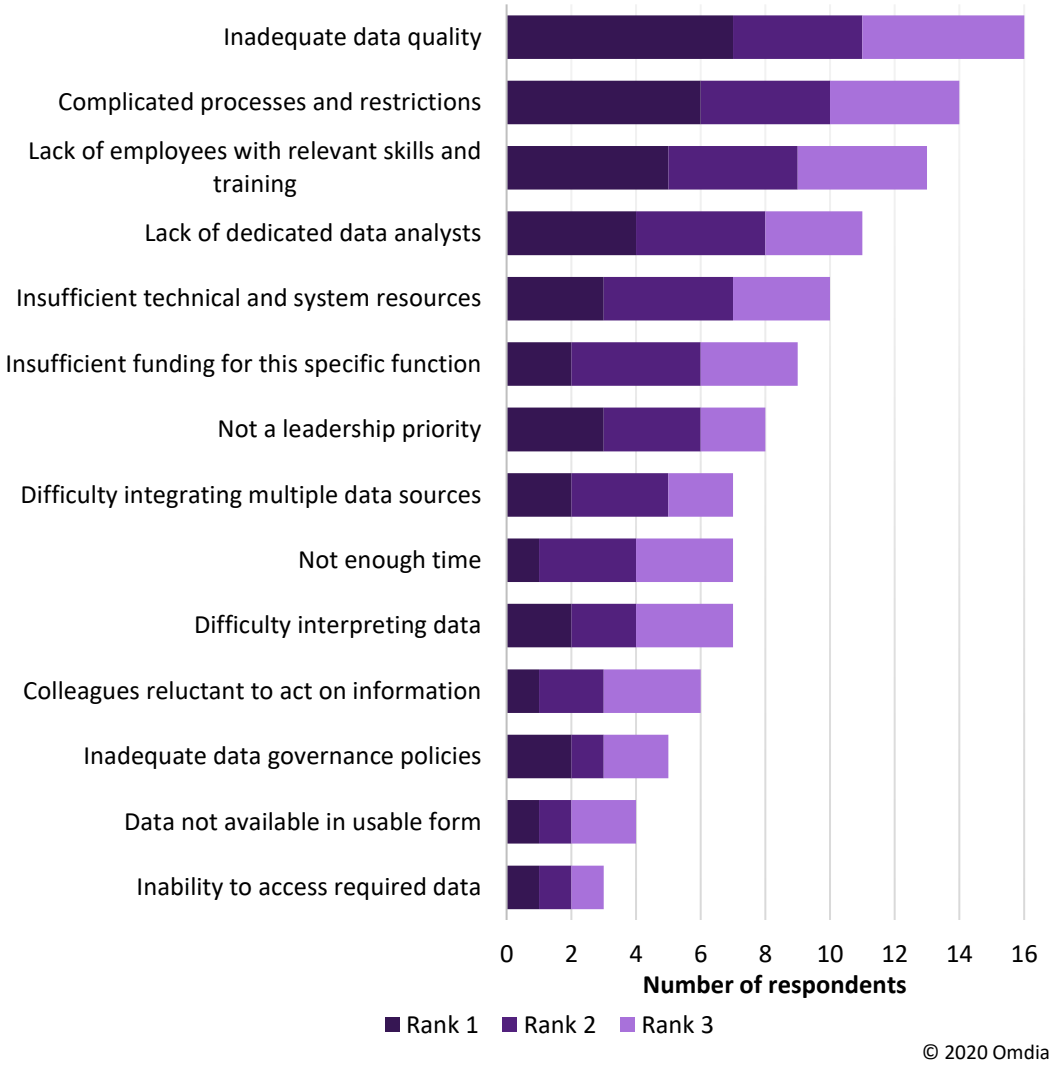
Figure 4: Big data challenges



Source: Omdia

When we look at challenges for analytics, the data governance and information architecture issues are exposed as inadequate data quality and complicated processes and restrictions. These issues are quickly followed by a lack of staff resources and skills. These are a logical extension of the information architecture and data governance shown above.

Figure 5: Top challenges for analytics

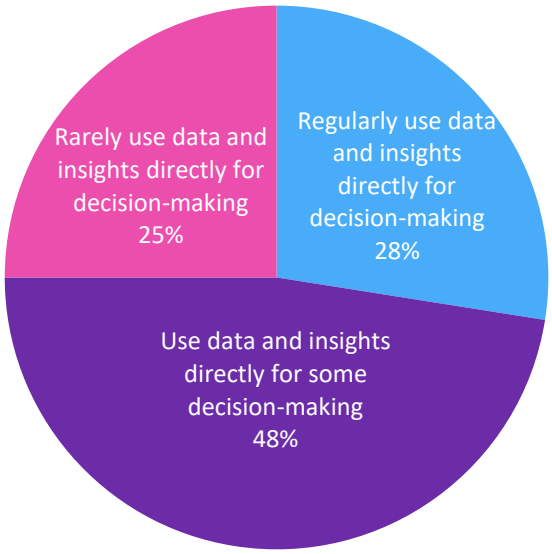


Source: Omdia

Interestingly, Figure 5 indicates that inability to access required data was the least of the challenges for agencies, indicating that it is an abundance of data rather than a lack of it that is an issue.

With this background of poor data quality, complicated governance processes, and lack of information architecture, it is not totally surprising that respondents indicated that only 28% of senior management regularly use data and insights for decision-making (Figure 6).

Figure 6: Senior management use of data and insights for decision-making



Source: Omdia

Omdia view

There appears to be an underlying lack of trust around the data and insights that are available to the senior levels of Australian government agencies. This is understandable because of the lack of underlying data quality and governance: they would be unsure of the accuracy, currency, and appropriateness of the data presented to them.

If a government agency's digital transformation is to be successful, organisations must pay greater attention to data platforms, to the automated use of data within their core processes, and to formalising the use of data in business decision-making.

Data platforms need to assist in identifying the data that an agency already holds, then characterise it for quality, use, sensitivity, and business value. These platforms should support data – whether it is in place, warehoused, or archived – equally and provide intelligent assistance to data owners and custodians. This foundational work can make government data available for use by other organisations and provide transparency to the public around data use and compliance. Good platforms will reduce the cost of discovering, storing, and governing data by applying AI, automation, and archival storage techniques.

Information management and governance products from Micro Focus can assist agencies in identifying, classifying, and securing structured and unstructured data and are able to provide a consistent approach for all data holdings within and agency.

Once the data is understood, the right data can be confidently used for analytics and derived insights. Flexible and scalable tools will be important to ensure these insights are

available when required and can be embedded into the organisation's decision-making processes.

The Vertica big analytics platform is a scalable, infrastructure-independent platform that supports time series and geospatial data with embedded machine learning capability, easily meeting the technology challenges around infrastructure scaling and analytics processing.

Rising use of AI and intelligent automation

AI and intelligent automation promise to remove time-consuming, repetitive, and error-prone processes, freeing public servants to perform more valuable and citizen-centric functions. Used as a force multiplier, they can increase an agency's effectiveness and responsiveness while also improving accuracy and consistency.

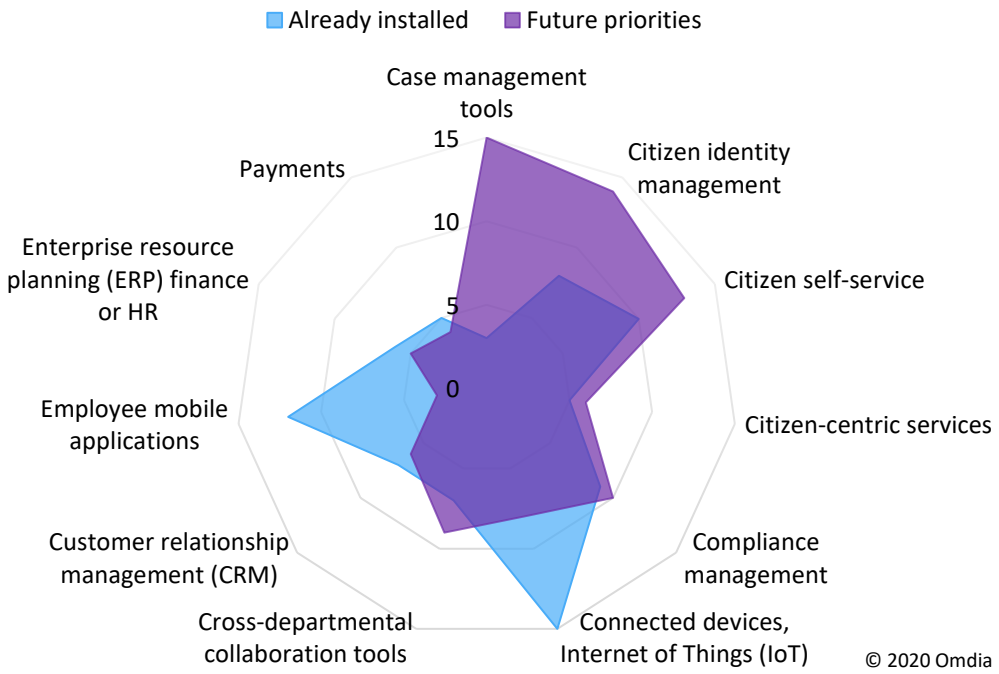
Artificial intelligence

When surveyed, 38% of respondents stated that their agency had no plans to implement AI. When they were questioned further it became clear that most were thinking of AI for critical decision-making and were concerned that "the level of transparency for government decision-making does not yet exist", and their "data is not ready for AI".

The agencies utilising or planning to deploy AI are aware that it comes in many forms and can support their business in multiple ways.

Agencies are following a cautious deployment approach by looking at internal solutions spaces before implementing citizen and consumer services dependent on AI. Current implementations, shown by the blue area in Figure 7, show a preference for internally focused deployments (bottom left), managing connected devices, and employee applications. There is now a movement from these safe deployments with internally focused outcomes to external, citizen-focused use cases, shown on the top right of the figure, including case management, citizen self-service, and identity management.

Figure 7: Shifting focus for future AI deployments



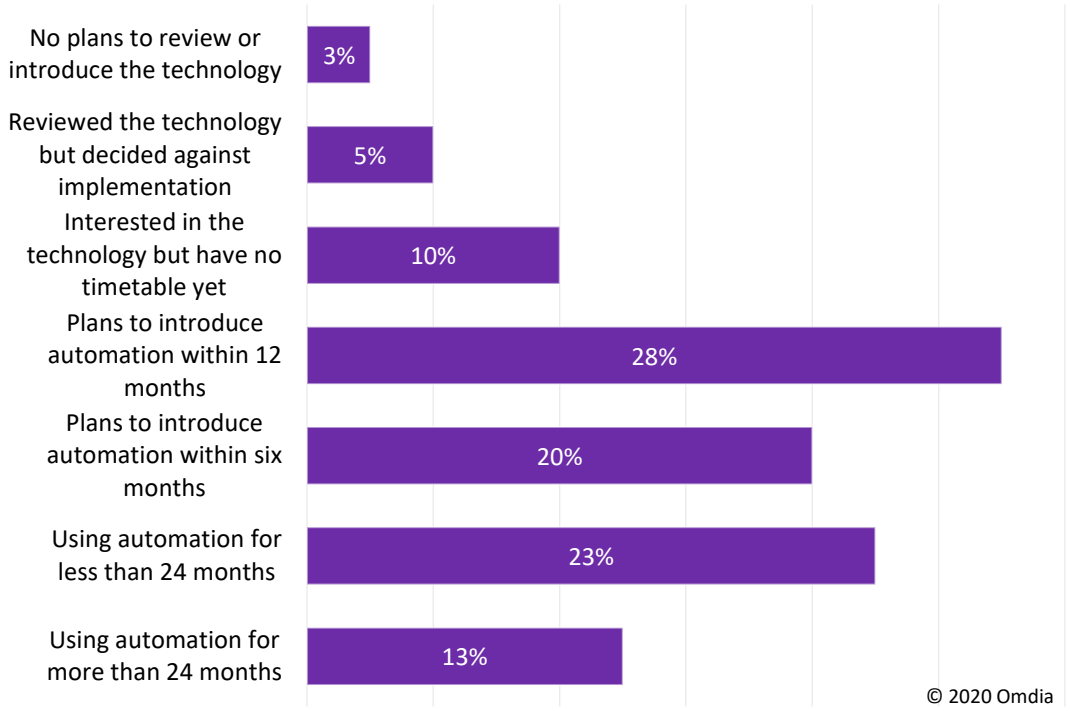
Source: Omdia

These future deployments will be focusing on natural language processing via contact centres, chatbots, and biometrics. Also, AI in case management will allow for the intelligent routing and escalation of cases and the presentation of relevant information to the caseworkers.

Automation

Omdia research shows that 36% of respondents stated they had already implemented automation technology in their environment, with another 48% indicating a planned investment within the current budget horizon.

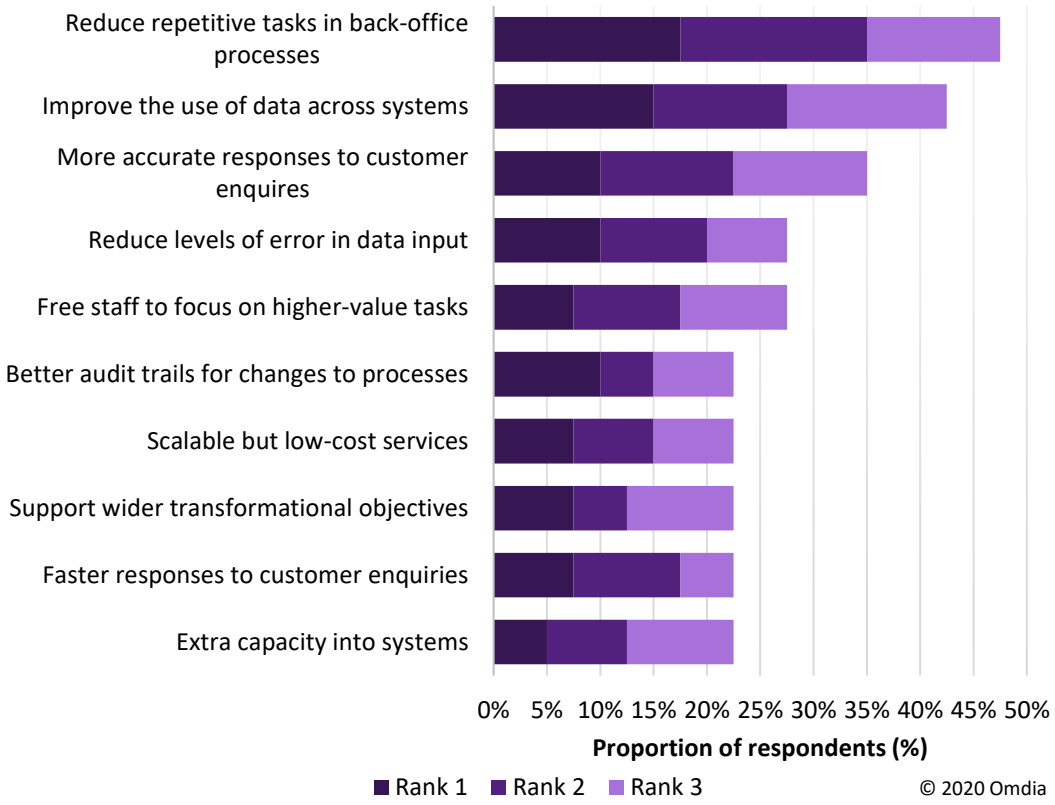
Figure 8: Current status of automation



Source: Omdia

The drivers for automation (Figure 9) to date are targeted at internal improvements around the back-office process and data usage and quality. The more strategic reasons, such as freeing staff for high-value tasks or supporting transformational objectives, are quite low down among responses.

Figure 9: Top reasons for automation



Source: Omdia

This internal-first approach reflects the cautious approach to technology implementations across government. It is important to ensure the agency and its staff understand and become familiar with the technology before rolling it out in external or high-profile projects.

The research also clearly reflects the desire to improve data quality within the agency to support analytics and AI.

Omdia view

A broader view of AI needs to be embraced by federal government agencies. AI-enhanced tools can be used to manage the increasing volume of unstructured and structured data. Data classification, discovery, and redaction and archive management can all be supported with natural language processing AI tools such as Micro Focus IDOL and Vertica.

Intelligent automation can also solve significant problems for agencies dealing with myriad systems supporting specific services and functions. As part of a broader transformation programme, they can be used to integrate legacy systems until they are modernised or replaced, remove tedious and error-prone work from staff, and provide a pathway for automatic resolution of many issues or tasks.

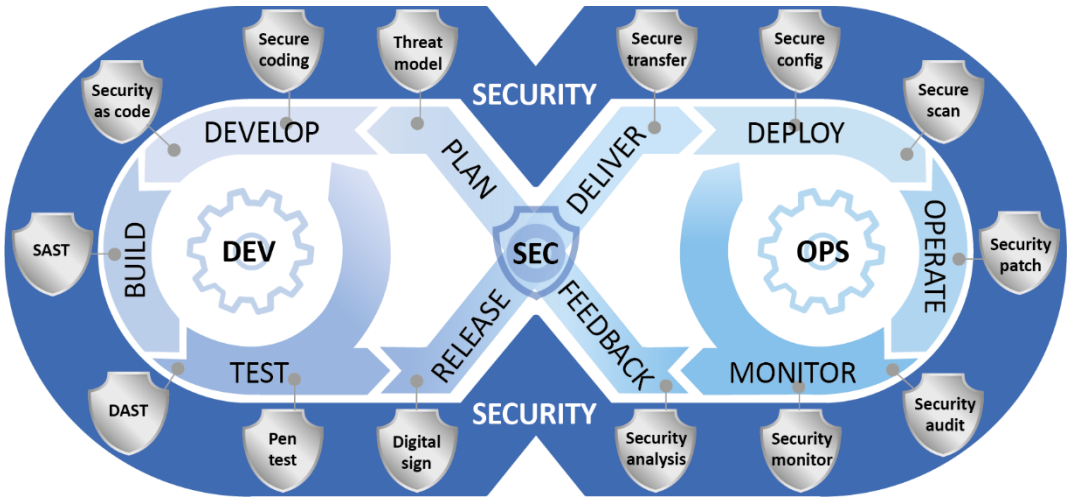
Agencies should be looking for products with AI and automation built in. IT service management (ITSM) and IT operations management (ITOM) can increase the effectiveness and efficiency of IT branches within government agencies, and investing in these intelligent systems will reap benefits. Micro Focus leverages its automation and AI technologies in its ITOM and ITSM products to provide intuitive and responsive service delivery.

Intelligent automation has the opportunity to refocus the workforce in government agencies onto the more relevant and more important aspects of their functions. In the shared services functions, it allows them to be more business focused, providing services and advice at a more personal level to the rest of the organisation. Staff in policy areas can spend less time collating and orchestrating information and input and more time engaging with the community and stakeholders. Service delivery areas can put the human touch into the equation, understanding the background and situation of each person they engage with. This does require the consideration of delegation within the service and a serious conversation about employee responsibilities to ensure staff are able to perform these higher functions.

DevSecOps practices to accelerate delivery

DevSecOps and Agile software development practices are a vital pillar of a responsive organisation. The ability to implement new programmes, payments, and conditions quickly and accurately while ensuring privacy and security is critical to delivering services to the public and supporting the government.

Figure 10: DevSecOps infinity loop



Source: US Department of Defense

DevSecOps aims to leverage the techniques of continuous integration, automated testing, and continuous deployment on the development side and infrastructure and security as code on the operations side to create a feedback loop where security, development, and operational teams and technology work together to deliver the services required.

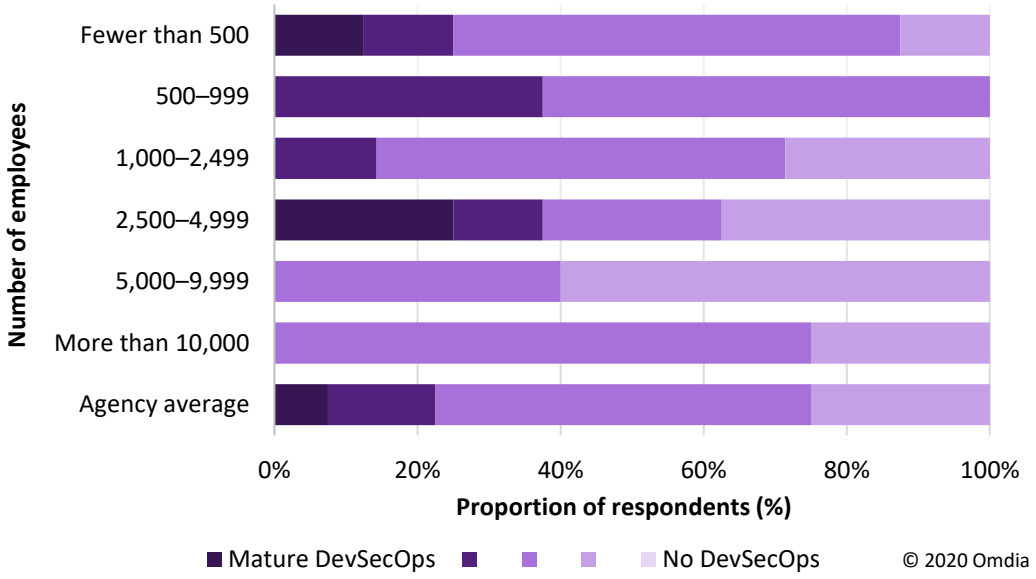
These modern delivery practices require organisational, cultural, and technical changes that are often difficult in larger organisations.

DevSecOps maturity

Our survey results show that Australian federal government agencies have not progressed very far on the implementation of DevSecOps, with 61% saying that their IT team structures were still technology centric. When asked about the usage of automation in their most mature DevSecOps teams, less than 1% had significant automation across the entire DevSecOps loop.

It was clear that significant steps toward automation exist in the governance, security, and risk areas, with 30% of respondents saying they had significant automation in those areas.

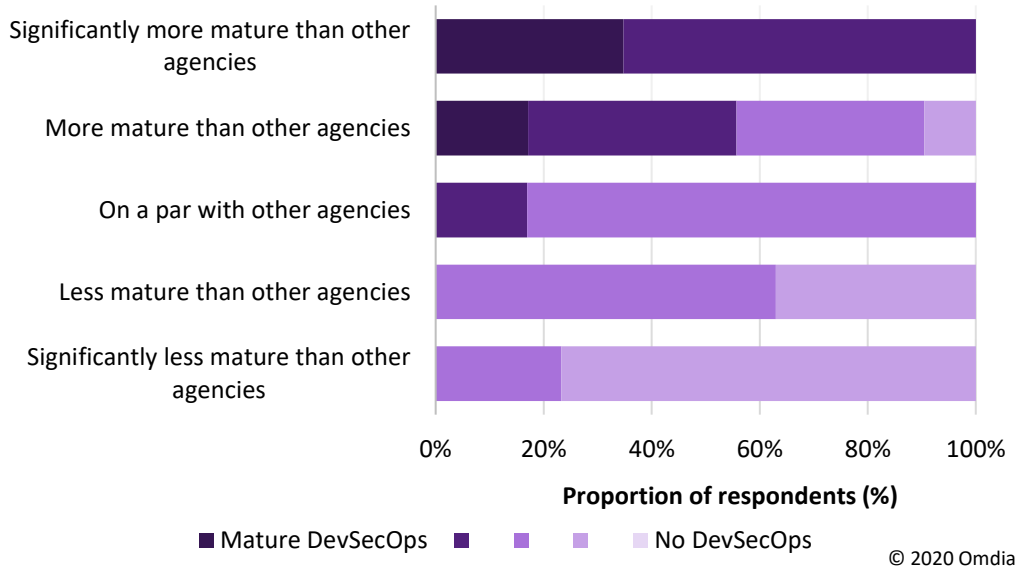
Figure 11: DevSecOps maturity by agency size



Source: Omdia

As shown in Figure 12, respondents are quite aware of their relative maturity against other agencies and clearly understand the challenges that face them.

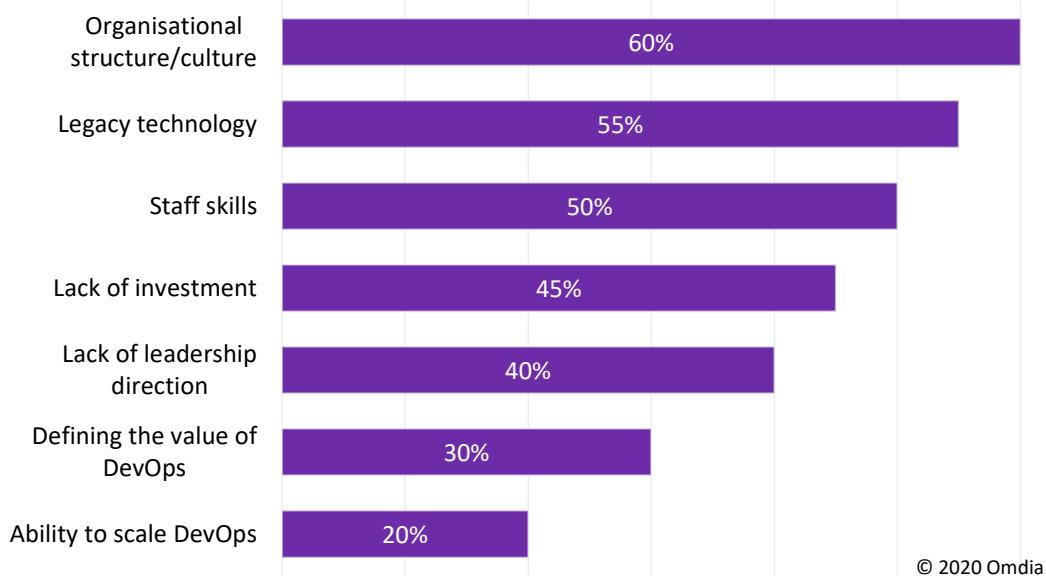
Figure 12: DevSecOps self-assessment



Source: Omdia

Respondents see that their culture and organisation structure is their biggest challenge, followed by legacy technology and staff skills (Figure 13). This is understandable with any significant change in practice. Overcoming this resistance requires clear direction and leadership from the executive and implementation and follow-through of a strong change management programme for the affected organisational areas.

Figure 13: Challenges in implementing DevSecOps



Source: Omdia

Omdia view

Government agencies have a long way to go in the adoption of DevSecOps. However, some pockets of excellence exist in some agencies. Work is starting on organisational structures, but significant challenges exist around legacy technology and the adoption of DevSecOps tools to automate and accelerate the practice. The survey and interviews show that many agencies are using the title *DevSecOps* without implementing the key principles, practices, and technology that it implies.

The survey reflects the perception that core systems built on legacy technology, specifically mainframes, cannot become part of the DevSecOps club because of the risk of change at a pace that DevSecOps advocates. New tools that provide access to a modern integrated development environment (IDE), smart editing and debugging, instant code compilation, and automated testing exist for legacy COBOL and PL/I applications. Along with current DevSecOps practices, they can create an agile development environment that will improve application maintenance and development efficiency without impacting quality and resilience.

Removing the perceived bottlenecks and siloed teams will allow departments to modernise legacy applications and enable them to operate within a distributed team across the department, delivering new releases faster, using Agile and DevSecOps practices at scale.

This approach will not only change the mainframe development team but allow for the integration of core legacy systems into the broader application portfolio, enabling agencies to isolate business logic into reusable components behind APIs and thus assisting in re-architecting systems and eliminating low-quality and redundant code.

These tools not only open the mainframe into a broader ecosystem but allow new developers to work on these systems without reverting to a 1990s workflow.

Integration and automation are vital aspects of a successful DevSecOps implementation, with operational monitoring driving automated responses and code driving automated testing and deployment. Agencies must look at the DevSecOps loop as a whole and ensure that their tools cover the breadth of systems, new and old.

Investment activity is being reprioritised

Research undertaken by Omdia shows that there is a significant planned investment in core IT management products to support digital transformation activities. Even considering the impacts of the COVID-19 pandemic, CIOs overwhelmingly agreed when interviewed that investment levels would not be fundamentally affected; however, priorities would be reassessed.

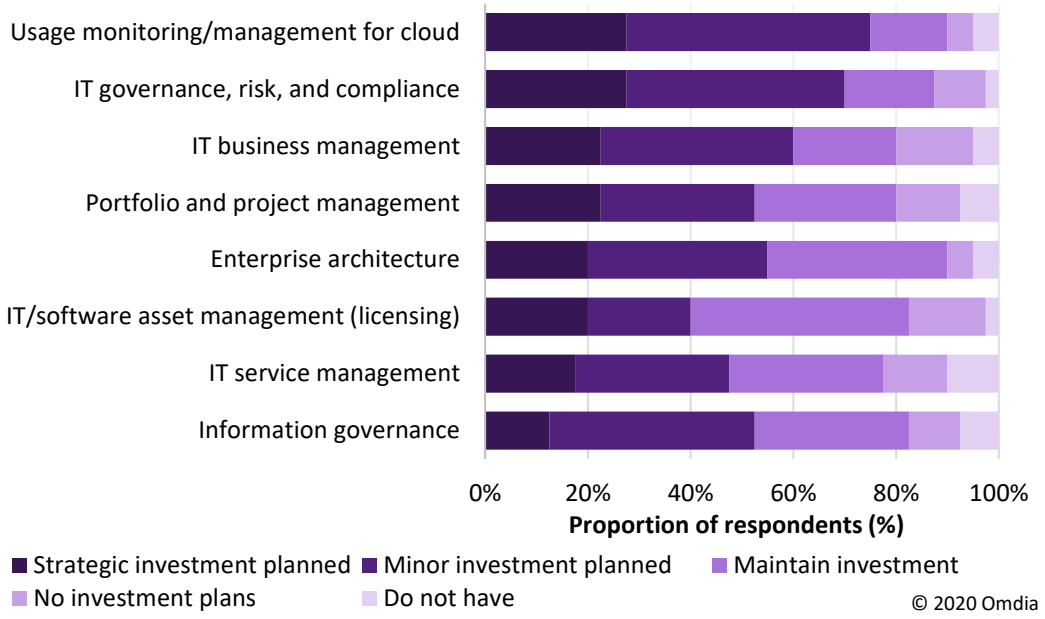
Investment in IT management

Investment in IT tooling can improve the delivery outcomes for many agencies across ITSM; enterprise architecture; and governance, risk, and compliance tools. Software technologies are required to ensure delivery of the appropriate services to business areas within the agencies.

Figure 14 shows that investment in cloud monitoring and management tools is a significant focus for many respondents, with 76% indicating an increased investment. This number reflects the underlying reality that more and more agencies are dependent on cloud services to deliver outcomes. Hand in hand with that is the significant investment in governance, risk, and compliance tools to ensure privacy and correct use of government data and systems.

IT business management tools take a holistic view of the business of IT within an organisation. Solutions are usually a collection of tools that cover every part of the IT function from demand to operations and everything in between, often following the Open Group's IT4IT architecture. Twenty-three per cent of respondents indicated a strategic investment in these tool sets.

Figure 14: IT investment priorities



Source: Omdia

Omdia view

The current and desired IT landscapes within government agencies can seem to be a universe apart, and continued investment in parts of the IT ecosystem without a strategic view of the whole is still the typical approach. Government agencies are trying to reach for the future while their feet are stuck in the mire of their current technologies.

Investment in tools that can span the existing legacy and on-site systems but also allow growth in investment in AI, automation, and data wherever it resides or executes will be the differentiator of those that succeed in overcoming their organisation's inertia. These tools can support new ways of working and, with the right leadership, shift the culture within an agency and help to address the significant challenges agencies know they face.

Leveraging technologies – such as those provided by Micro Focus – that allow agencies to extract value from existing investments while opening new opportunities and business operations will enable them to innovate incrementally. Micro Focus recognises that organisations must "run and transform" their existing portfolio while also "innovating faster with lower risk". It builds products with the aim that they are "built on stability, innovation, and delivering for customers over the long term".

IT tooling with the highest flexibility will have the greatest value. Look for flexible deployment options across on-site, private cloud, or public cloud; flexible integration through APIs; and an extensive ecosystem of vendors and service providers to ensure that the products can support where you are now on your transformation journey and where you will be in the future.

Appendix

Further reading

ANU Poll 2018: Data Governance (February 2019) Available at <https://dataverse.ada.edu.au/dataset.xhtml?persistentId=doi:10.26193/XHORAI> [Accessed December 2019]

Methodology

Omdia undertook a 35-question survey of technology decision-makers and influencers within Australian federal government agencies. We received 40 responses with a 45/55 split between decision-makers and influencers, with a good spread across all agency sizes.

After the survey responses were analysed, five one-on-one interviews were undertaken with CIOs from a variety of departments and agencies to explore some details further.

Author

Tony Castley
Principal Analyst, Enterprise ICT Management
tony.castley@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalise on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About [partner company]

Micro Focus is one of the world's largest enterprise software providers. It helps customers digitally transform their organisation and achieve the speed, agility, security, and insights necessary to succeed in today's rapidly evolving marketplace. By design, its solutions bridge the gap between existing and emerging technologies – enabling faster innovation, with less risk, in the race to digital transformation.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, and agents disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.