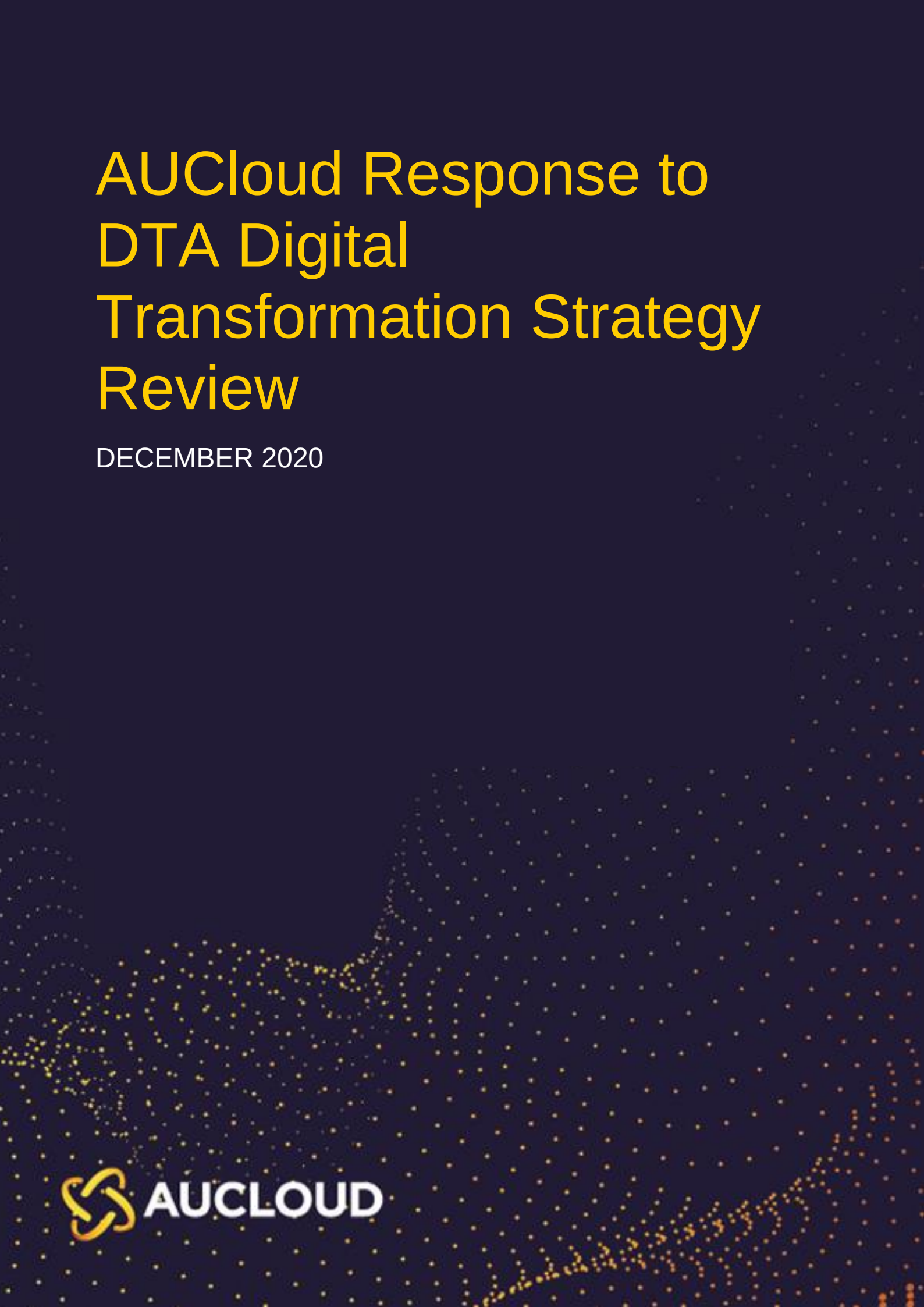
AUCloud Response to DTA Digital Transformation Strategy Review

DECEMBER 2020



Disclaimer

The information in this Proposal is the confidential information of Sovereign Cloud Australia Pty Ltd ("AUCloud"). Such information must confidential at all times and used solely to consider the Proposal put forth by AUCloud. You agree to take such measures to prevent the disclosure of the information as you would to prevent the disclosure of your own proprietary information, but in all cases, shall use at least reasonable care.

You do not acquire any rights in the information. All AUCloud trademarks and logos belong to Sovereign Cloud Australia Pty Ltd. Other trademarks and logos belong to their respective owners and are used for informational purposes only.

The contents of this document constitute valuable proprietary and confidential property of AUCloud and are provided subject to specific obligations of confidentiality set forth in one or more binding legal agreements. Any use of this material is limited strictly to the uses specifically authorised in the applicable license agreement(s) pursuant to which such material has been furnished. In the event there are no applicable license agreement(s) governing the use of this material, please be advised that any use, dissemination, distribution, copying or disclosure of all or any part of this material not specifically authorised in writing by AUCloud in advance is strictly prohibited.

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, AUCloud's response may include information about solutions or products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. AUCloud is under no obligation to provide such future functionality.

As the rate of transformation accelerates in the next 5 years, are there additional principles that we should elevate in the next iteration of the Strategy? Principles may cover privacy, cyber security and data retention.

A key learning of the last 12 months on the back of bushfires, floods, droughts and a world that has literally 'shut-down' as a result of Covid-19 is that we need to ensure we are in better shape to cope with whatever might be round the next corner. Whatever the business of government, there is a need for greater sovereign resilience. This is NOT about protectionism or isolationism but building sovereign capability – including within government. It is about prioritising investment in strengthening Australia's self-determination, improving our ability to adapt and respond rapidly and maturing the sophistication of how we assess and mitigate risk.

With this in mind, we believe that **building sovereign resilience**, must be a foundational principle upon which the next iteration of the Government's Digital Transformation Strategy is built. This translates to a focus on building sovereign capability to enable greater self-determination, adaptability and effective risk mitigation investment to ensure we have the ability to rapidly pivot and respond to changing and unforeseen circumstances – as well as, and just as importantly, policy and service changes that meet the needs of citizens.

An equally important additional principle is **increased transparency.** Public belief that the 'right thing' is being done in the right way for the right reasons will always trump the cynical instincts of commentators. Take the COVIDsafe App released by the DTA. Extraordinary efforts were made to ensure transparency to mitigate privacy concerns around the *perceived* invasive tracking capability of the application to deliver an effective solution against the clock. Security and privacy by design were key aspects of the application development and the intent of transparency clear through the release of source code, the Privacy Impact Assessment and supporting privacy legislation.

The Government is welcoming feedback on the opportunities and areas of focus for data and digital initiatives that would deliver the best outcomes in assisting with promoting jobs and return to growth.

On the back of a very tough 2020 – and as it looks to the future use of digital technologies, Government is facing three pressing imperatives. These include the need to:

- be more cost efficient through doing more with less;
- reduce wasteful, expensive and time-consuming redundant activities to deliver tangible value more quickly – time to value; and
- increase transparency to foster and sustain trust.

Nothing is more powerful in today's fast paced, mission critical world than digital native (containerised micro-services) applications based on cloud services to deliver against these drivers.

First, cloud services compress massive inefficiencies from traditional approaches through:

- Economies of scale (across both supply and demand) that improve asset utilisation;
- DevSecOps orientated automation and orchestration; and
- Standardisation of design and operations.

Significant efficiencies can be achieved across the end-to-end digital native design, development, deployment and operating cycle, freeing up resources and delivering savings that can be targeted to more innovative and/or citizen centric endeavours that deliver better service outcomes for individuals and communities.

Second, driven by a framework of standardisation, speed to market and iteration, digital native applications on cloud provides orders of magnitude improvement in *time to value*, i.e., delivery of the service/outcome more quickly with benefits realised sooner.

Finally, the economics of the cloud service model is (or should be) inherently transparent. On the supply side, because the buying power of cloud providers reduces their unit costs, they can pass these savings on to customers – buying big delivers the cost efficiencies that come with economies of scale. On the demand side, higher utilisation of the infrastructure assets of cloud providers, similarly drives costs down, which again, can be passed on to customers. Importantly, cloud enables the alignment of technology utilisation with the demand patterns of end users; you only use what you need and pay for what you use. You pay more as you use more. And when you use less, you pay less. You can scale up and down to meet your need and you don't pay for what you don't use.

These features – inherent to cloud services, translate to the ability to be more agile; to do more, more quickly; de-risk and hence stimulate innovation; and ultimately, realise benefits sooner. These benefits flow directly to government in terms of efficient, effective and quality services to citizens and businesses who can leverage government support to drive opportunities for self-reliance and ultimately growth and jobs.

In order to deliver simple, helpful, transparent and respectful services for our users, Government is interested in exploring what opportunities exist for greater reuse of capabilities across government.

Core to the next iteration of the Strategy is the desire to be more adaptive and to accelerate change. The significant progress government has made in defining a whole of government architecture that supports the standardisation of technology approaches is a crucial foundation for the sharing and reuse of capabilities – as opposed to the longstanding tendency to design and build bespoke solutions.

Critical to the success and cost effectiveness of the government's intended platforms-based strategy is that any solution facilitates further scalability, adaptability and innovation. To this end, the architecture must avoid the risk of monopoly through lack of interoperability. Further, the architecture must insist on full transparency to control, as required, the movement of citizen data (metadata, support data, analytics data etc) where there is the risk of it being inappropriately moved, including offshore.

Digital standards are good, but government must also mature its understanding of how to effectively use and transition to, cloud-based services. This includes the respective pros and cons of transitioning legacy-based systems to cloud as opposed to developing and deploying cloud native applications through standardised IaaS and microservice, containerised APIs.

For the Strategy to embed agility and innovation in the future design and delivery of services and capability, moving to standardised cloud native IaaS, PaaS and SaaS must be the goal.

As described below there are Four Stages of Cloud Maturity. While stages one and two deliver some of the inherent benefits of cloud technology, it is at stages three and four that the agility, flexibility, efficiency and innovation government aspires to, is exponentially realised.

STAGE	CHARACTERISTICS
Stage One: Legacy Workloads	• Single tenanted applications operating on mix of physical and virtual estates. • Asset under-utilization at all levels (data centre, network, compute and storage). • Lack of automation, orchestration and monitoring. • Inflexible operations as a result of buyer procuring bespoke proprietary vendor technology and disparate outsourcing arrangements (change management technically challenging and contractually costly). • Complex protocols for integration with external parties (less about alignment of technical protocols and more about harmonisation and agreement on security and privacy policies when sharing access to data).
Stage Two: Cloud Hosted workloads	• Workloads/Apps Hosted on cloud IaaS • Hosted in an environment that can be accessed via a portal or API • Access to flexible commercials, providing pay as you use billing based on hourly consumption. • Some automation, orchestration and monitoring functionality available that can be integrated into standard operating procedures to improve security posture, availability management and overall service delivery *Typically: key function of cloud hosted applications is that they are a re-deployment or hybrid adjunct of existing single tenanted applications. They have not been re-architected to utilize the wide range of automated and integrated functionality inherent within NIST IaaS or PaaS.*
Stage Three: Cloud Native Workloads	Applications and services have been re-architected to maximise the inherent and unique capabilities offered through cloud computing: e.g., self service, API-driven. Enables: • on demand scalability • API centric, containerised, microservice applications – ability to package up applications and their dependencies separately. Applications can be built more quickly and deployed independently and in increments • integrated Dev/SecOps risk mitigation • applications and components to drive increased flexibility and agility • API interoperability with other IaaS providers • flexible standard commercials.
Stage Four: Digital Native Workloads	Supports API integrations with Platforms (PaaS) – allowing customers to develop, run and manage Web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an App. Applications can be redesigned to match workflow requirements and fully integrate with PaaS and leverage the functionality of PaaS.

A day to day challenge for many CIOs is that the maturity of cloud adoption and the technical and cultural 'journey' it requires, are not well understood. It is imperative that the Strategy establish the right framework, foundations, standards and definitions from the outset to avoid vendor lock in and facilitate the full technical, capability and commercial flexibility available through cloud native IaaS, PaaS and SaaS. Agencies need a clear and unambiguous pathway that facilitates the benefits outlined above (Stages 3 and 4) and achievement of the agility, innovation and speed to market government is committed to achieving.

Government is seeking feedback on best practice co-design approaches that can deliver ambitious outcomes at a whole of government or whole of nation level.

Understanding and leveraging the flexibility and agility of cloud native platforms is an area government could derive significant long-term benefits. How to do this, the associated journey and practical design path is a clear opportunity for co-design - and skills sharing and transfer.

Government is interested in better practice examples of how to further embed innovation to securely deliver faster, simpler and tailored experiences for users.

Driven by a framework of standardisation, speed to market and iteration, digital native applications on cloud IaaS provides orders of magnitude improvement in innovation and time to value, i.e., delivery of the service/outcome more quickly with benefits realised sooner.

Cloud both accelerates and de-risks innovation; ideas can be tested quickly, without expensive physical infrastructure. Cheaper innovation is less risky, easier to justify and enables you to achieve more with the same budget. Leveraging cloud microservice, containerised APIs, enables a flexible and agile approach to testing 'new ideas' with the cost of iteration and failure substantially reduced. Cloud native IaaS provides the foundation to support innovative PaaS and SaaS solutions and new operating and delivery models that are otherwise resource and time intensive and, as a result, too costly to fail.

The Government is interested in exploring how others have achieved true agility and what lessons can be taken from the private sector.

As a sovereign cloud IaaS provider our business is premised on agility. This includes our ability to respond, architect and design IaaS services that incorporate the latest technology developments as well as the ability to deliver an agile on-demand IaaS model that provides the flexibility and scalability our customers and partner community need to meet their requirements at any point in time.

Of equal importance is the ability of cloud IaaS platforms have to continuously improve, including 'hardening' security as the cyber threat landscape changes. Indeed, this should be core to the agility of providers premised on standardised cloud-based services. This is, in large part, the result of building a genuine NIST based cloud IaaS which inherently delivers agility through provision of:

- on demand services;
- broad network access (multiple services, multiple devices from multiple locations);
- resource pooling (infrastructure, networking, security etc to achieve efficiencies, without compromising security);
- rapid elasticity (to scale demand up and down as required); and
- metering capability, i.e., the ability to fully and transparently monitor what you use.

By way of example, AUCloud's delivery of a Virtual Desktop as a Service Solution to the ANU during Covid demonstrated the clear agility and flexibility of leveraging a standardised, NIST based cloud platform – in this case, cloud IaaS.

When stage three lockdown measures came into place in March 2020, the ANU needed to quickly transition students, staff and lecturers to a remote platform with the same level of access to campus-based resources and functionality. In just one week, AUCloud implemented a turnkey solution that allowed the University to move its operations online, with the capacity to scale to support over 20,000 students, including international students located overseas. Feedback from the ANU on AUCloud's design through to deployment of the solution, compared with a traditionally managed and built solution, was that an otherwise six months project was delivered and operational in six days. This isn't just about reduced costs from charging services over a shorter timescale but the five month and 24 days of additional time that the project outcome is operational and used (and the value that creates) as well as the earlier delivery of other projects dependent on its deployment.

Government is looking for examples of new and innovative approaches to digital service delivery that would achieve better outcomes for the people of Australia.

Over the last 18 months government has made important progress addressing the issues of security and privacy within a digital context. As noted above, in releasing the COVIDsafe App the DTA took extraordinary efforts to ensure transparency to mitigate privacy concerns. The work by ACSC in developing the new Cloud Assessment and Authorisation Framework similarly focuses on the primacy of security as it relates to data management and protection.

A key area yet to reflect the agility, transparency, value and speed to market that underpins the Digital Transformation Strategy is procurement. The procurement process continues to confuse buyers and suppliers alike, is not sufficiently transparent to avoid being 'gamed' and is not conducive to competitively driven speed to market. The existing Digital and Cloud Marketplaces remain cumbersome (despite the best of intentions) and does not take advantage of some of the commodity type services offered through cloud.

We recommend that the Cloud Marketplace should, by default, be the place where NIST based cloud IaaS services can be purchased 'off the shelf' with full price, capability and service transparency. Transparent markets with clear rules and visibility of inputs and outputs are by nature efficient. Take for example the Australian Stock Exchange (ASX) model; all price and service inputs and outputs are public, with full transparency governed by clear rules and protocols dictated by the marketplace (ie ASX and the trading market). The model is inherently low friction, hence low transaction costs, supported by market rules and compliance requirements that require transparency and full disclosure to drive competitiveness and value. Poor performance and lack of transparency drive lack of confidence and downturn of results. The incentive to improve and remain competitive is driven by the market and rules that dictate its operation. This same model equally applies to cloud-based commodity type services - all players can be on an equal footing with comparable offerings in a competitive market.

Government is interested in innovative ways to overcome the policy barriers to achieving digital transformation.

Two areas of policy need to be addressed. The first is agile procurement; how to address this was discussed above.

The second is an agreed definition of data that applies consistently across government and government information including in the context of procurement, policy and legislative documentation/requirements. A consistent definition of data is critical because it provides an unequivocal, standardised understanding that can be applied to the management and protection of 'data' in any digital context – consistently. This is imperative to ensuring government can compare 'like for like' service offerings and the transparency and rigour of security protections and mitigations, including where the data of Australian citizens may move offshore.

In assessing the risks associated with cloud providers, the ACSC clarified earlier this year that data in a digital context is not simply 'customer data' but includes account data, metadata, support and administrative data. To avoid confusion, ensure consistency and facilitate clarity of policy and policy execution, this definition should be applied across government.

Government is keen to explore innovative models and approaches to stakeholder engagement that lead to better outcomes.

Part of getting better outcomes is growing Australia's digital capability through raising ambitions, removing friction and widening market opportunities for those digital and technology related SMEs that have the

ambition, capacity and capability to grow their business not only in the Australian domestic market but also to scale up into global exporters and operators. Not all SMEs owners have or even want this for their business.

However, in engaging with stakeholders, specifically vendors and service providers, it would serve the growth ambitions of government to understand where these opportunities are and how it can support these (already proven) businesses to scale to drive more jobs and more revenue.

General comments

Simply reflecting on the utilisation of cloud and digital standardisation, security and the value of scaling rapidly to meet unpredictable demand during Covid, it is clear the focus on digital has driven a wrecking ball through any cultural desire to pontificate. This is no longer just an aspiration. The events of the last 12 months have fully demonstrated both the need for digital technology to enable agility as well as its ability to deliver.