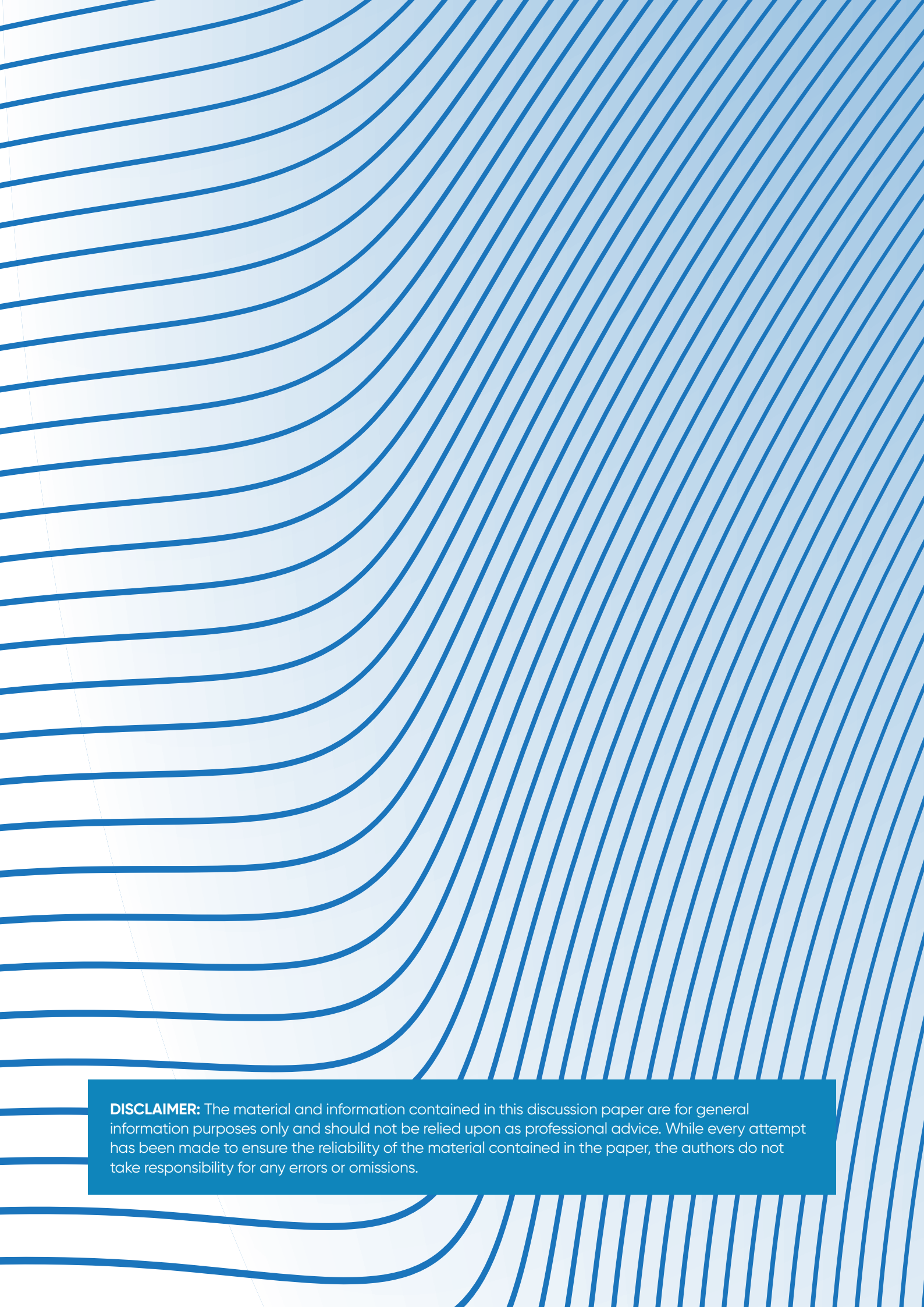


The background of the entire page is a solid blue color with a pattern of thin, white, wavy lines that create a sense of depth and movement, resembling a topographical map or a stylized cloud pattern.

CLOUD CONTROL

**What the cloud is, what it does
and how it can be securely adopted**



DISCLAIMER: The material and information contained in this discussion paper are for general information purposes only and should not be relied upon as professional advice. While every attempt has been made to ensure the reliability of the material contained in the paper, the authors do not take responsibility for any errors or omissions.

INTRODUCTION

Cloud technologies are widely used, benefitting all sectors of the Australian economy. But there is a widespread lack of common understanding, including among Australia's policy makers, as to *what* the cloud is, *what* it does and *how* it can be safely and securely adopted.

Policy development to help leverage cloud capability in Australia has failed to keep pace with cloud technologies. Ultimately, this adversely impacts our nation's interests because these technologies, if fully realised and implemented, have transformative potential. This is especially pertinent in relation to cyber security, as cloud capabilities increasingly support economic activity, society, government service delivery and national defence. Cloud adoption must also form the cornerstone of any policy aimed at driving and enhancing Australia's digital economy, which is a central focus of the 2021-22 Federal Budget.

Recognising the significant benefit that widespread cloud adoption can bring to the nation, the Federal Government has included certain cloud infrastructure and services as critical infrastructure assets in current legislative efforts to reform the security of critical infrastructure. Thus, the time is ripe for policymakers to truly understand and harness the power of the cloud to support the secure delivery of services to all Australians.

This discussion paper will:



Define the cloud along with its key applications;



Explore how innovations in the cloud can facilitate and support cyber security uplift across the Australian economy; and



Discuss recent developments in cloud technology and highlight future trends;



Identify issues and gaps in Australia's existing policies, regulation and frameworks that apply to cloud technologies and how they can be remedied.



CASE STUDY: NSW Rural Fire Service

Following the devastating 2019-20 bushfires the NSW Rural Fire Service (NSW RFS) harnessed cloud technologies to develop advanced analytics and planning. This cloud-based solution has accelerated the NSW RFS's ability to make data-driven decisions in emergencies and enhanced the effective management of frontline operations. In addition, cloud native interactive analytics dashboards provide insights for collaborative capability and capacity planning through to deployment, ensuring effective management of frontline operations.

WHAT IS THE CLOUD?

For many, 'the cloud' is an esoteric concept. Because it can't be seen it is intangible. In reality, however, it plays a role in the daily lives of almost all Australians, from service delivery, to work, to home. It is a part of everyday life. The great strength of cloud is that it enables a vast range of ubiquitous functions, from the simple to the highly complex. This is in contrast to more traditional on-premise security, data storage and ICT management. While on-premise may be more suitable in some cases, it requires significant investment, with onsite infrastructure and servers equating to additional costs for maintenance, upgrades and general operation.

The United States' National Institute of Standards and Technology (NIST) – the most commonly recognised global cyber security framework – defines cloud computing as:

"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."¹

Put in the most basic of terms, this means the cloud is unlike traditional approaches to data and IT system management, where organisations purchase, install, configure and operate software on their own infrastructure. Instead, all these services can be easily accessed, in real time, on the internet as a ubiquitous service. Hence, the use of cloud technologies and techniques provides the agility, flexibility, scalability and robustness required to operate in a digital environment.² Furthermore, the flexibility of cloud teamed with advances in technology means any organisation, from an SME to a national government, can be hosted and supported anywhere in the world, regardless of geographical and jurisdictional considerations. Because the cloud provider is doing the heavy lifting, services are more scalable and therefore easier for consumers to access, reducing complexity, risks and cost.

Cloud operates on a shared responsibility model and is dependent on the services used, infrastructure and tenancy. Ultimately, this means security and compliance is shared between the provider and client. The provider protects the infrastructure through which cloud services operate including hardware, software, networking and facilities, while shared responsibilities include security management via patching and configuration. For this model to work effectively, the security of data classification, network controls and physical security need to be clearly defined.³



1. [Cloud Computing | CSRC \(nist.gov\)](#)

2. [Secure Cloud Strategy \(amazonaws.com\)](#)

3. [Shared Responsibility for Cloud Security: What You Need to Know \(cisecurity.org\)](#)

NIST has specified five characteristics of cloud computing:

1. **On-demand self-service:** the use of a website or similar interface by consumers to manage computing resources without interaction between the consumer and the vendor.
2. **Broad network access:** facilitates network access to a broad range of connected computing devices.
3. **Resource pooling:** vendors use shared computing resources to provide cloud services to multiple customers, with virtualisation used to segregate and protect customer data.
4. **Rapid elasticity:** facilitates fast and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth.
5. **Pay-per-use measured service:** means customers only pay for the resources they use and are able to monitor their usage.⁴

There are three cloud service models. These are:

1. **Infrastructure as a Service (IaaS):** The vendor provides the physical computer hardware including CPU processing, memory, data storage and network connectivity, which is shared among 'multiple tenants' using virtualisation software. This allows customers to run operating systems and software applications of their choice, with the vendor typically controlling and maintaining the physical computer hardware and the consumer controlling and maintaining the operating systems and software applications.
2. **Platform as a Service (PaaS):** The vendor provides IaaS as well as operating systems and server applications, allowing customers to use the vendor's cloud infrastructure to deploy web applications and other consumer-developed software using supported programming languages. Physical computer hardware, operating systems and server applications are maintained by the vendor and the consumer controls and maintains the software applications they have developed.
3. **Software as a Service (SaaS):** The vendor's cloud infrastructure and platforms are used to provide customers with software applications, for example, email and file sharing. These applications are usually accessed via a web browser, meaning there is no need for the installation or maintenance of additional software. Physical computer hardware, operating systems and software applications are controlled and maintained by the vendor, with the consumer only controlling and maintaining limited user-specific application configuration settings.⁵

There are four cloud deployment models. These are:

1. **Public cloud:** This model involves the use of a vendor's cloud infrastructure, which is shared via the internet with multiple organisations and members of the public. It offers the benefit of cost efficiencies due to its scale but also has inherent security risks.
2. **Private cloud:** This model involves the exclusive use of cloud infrastructure and services located at an organisation's premises or offsite, which is managed by the organisation or a vendor. While it does not offer the same cost efficiencies, it does have reduced potential security risks.
3. **Community cloud:** This model involves the use of a private cloud shared by several organisations with similar security, storage and data processing requirements. The aim is to glean the security benefits of a private cloud and greater cost efficiencies.
4. **Hybrid cloud:** This model involves a combination of cloud models, for example, combines a private cloud with one or more public cloud services, with proprietary software enabling communication between the distinct services.⁶

4. [Cloud Computing Security Considerations | Cyber.gov.au](#)

5. Ibid 4

6. Ibid 4

FIVE ESSENTIAL CHARACTERISTICS OF CLOUD



On-demand self-service



Broad network access



Resource pooling



Rapid elasticity



Measured service

THREE SERVICE MODELS OF CLOUD



Cloud Infrastructure as a Service



Cloud Platform as a Service



Cloud Software as a Service

FOUR DEPLOYMENT MODELS OF CLOUD



Public cloud



Private cloud



Community cloud



Hybrid cloud



CASE STUDY: RedZed

RedZed provides a combination of residential and commercial mortgages to more than 6,000 self-employed Australians. The company's loan book has grown significantly in recent years, demanding a scalable and flexible infrastructure solution to support future growth. With the ambition of becoming the largest provider of financial services for the self-employed in Australia, RedZed needed a cloud-based banking platform that was easy to implement and use. It also had to meet its regulatory requirements. The company led with a cloud solution because it reduced processing time for mortgage applications and improved response time to customer enquiries; streamlined the process of assessing, identifying and originating mortgage loans in the platform for brokers; provided the senior management team with real-time updates on business performance, resulting in timely responses to the needs of investors and regulators; and enabled deployment within six months.

CLOUD PROS

- ✔ **Potentially reduced IT expenditure**
- ✔ **Scalability and flexibility to suit specific business needs**
- ✔ **Data is backed up and updates are automatic, enhancing data security**
- ✔ **Business agility and ease of collaboration**
- ✔ **Improved work flexibility**

CLOUD CONS

- ✘ **Potential cyber security risks due to poor controls**
- ✘ **Dependence on reliable, fast internet**
- ✘ **Reliance on vendor for technical support**
- ✘ **Cost can be prohibitive depending on specific needs**
- ✘ **Lack of flexibility of some cloud apps**

FUTURE PERSPECTIVES: WHERE IS CLOUD TECHNOLOGY HEADING?

The cloud is going vertical

A vertical cloud is optimised for a specific industry, or 'vertical', with more niche requirements regarding security and compliance. To achieve this, cloud providers develop and offer functions to meet industry-specific requirements and best-use applications, with the ultimate goal of streamlining the online functions and security needs of unique sectors to drive productivity and growth.⁷ Good examples of such vertical sectors include government, financial services, health and critical infrastructure.

AI and machine learning will improve scalability and automation

By harnessing the opportunities AI and machine learning present, cloud will drive scalability and automation, improving productivity and efficiency. Because of the scalability of cloud across a diverse cross-section of the economy, the deployment of technologies like image recognition, language processing and recommendation engines will see these cutting-edge tools being used more widely across the economy, bringing efficiency gains and automation benefits.⁸

Multi-cloud strategies

Businesses are moving towards the adoption of multi-cloud strategies, helping increase agility and flexibility, minimising vendor lock-in, taking advantage of a variety of cloud solutions and improving cost effectiveness.⁹ A multi-cloud strategy also offers the ability to select different services or features from different providers, which is advantageous as some cloud environments are better than others for specific tasks.

Move to the Edge

Edge cloud means reduced latency, lower costs and better cyber security for organisations. Leveraging the edge allows organisations to store sensitive information closer to the source, for example onshore as opposed to offshore, which not only means that governments can exert greater jurisdictional control, but also that data can be retrieved and accessed more quickly. Combining edge and cloud, harnesses the power of distributed systems, allowing the processing of data on a device itself, which then sends it to the cloud, where it can be processed, analysed or saved using less processing power.¹⁰ A good example of how the edge works is the case of online streaming services, which require the rapid retrieval of significant amounts of data. By storing this data on the edge hosted via micro data centres, increased transmission speed equates to better viewing.

7. [The Future Of Cloud Is Vertical \(forbes.com\)](https://www.forbes.com)

8. [The 5 Biggest Cloud Computing Trends In 2021 \(forbes.com\)](https://www.forbes.com)

9. [Multicloud: Everything you need to know about the biggest trend in cloud computing | ZDNet](https://www.zdnet.com)

10. [What is Edge Cloud \(Computing\)? | Infradata](https://www.infradata.com)



CASE STUDY: Taronga Conservation Society Australia

Over its 100-year history, Taronga Conservation Society Australia has evolved in form and function, from an entertainment hub to a mature conservation, research and education provider. Recognising the innovative edge that digital transformation brings to the organisation, particularly concerning wildlife conservation and the enhancement of visitor experience, Taronga has adopted a cloud-first strategy. Leveraging cloud technologies, Taronga has transitioned core business systems for HR, finance, and procurement; simplified secure access to core functions and content from any device with corporate credentials; and improved productivity through increased automation of daily administrative tasks, enabling staff to focus on more important activities such as animal care and visitors.

HOW CAN CLOUD TECHNOLOGIES LIFT AUSTRALIA'S CYBER SECURITY?

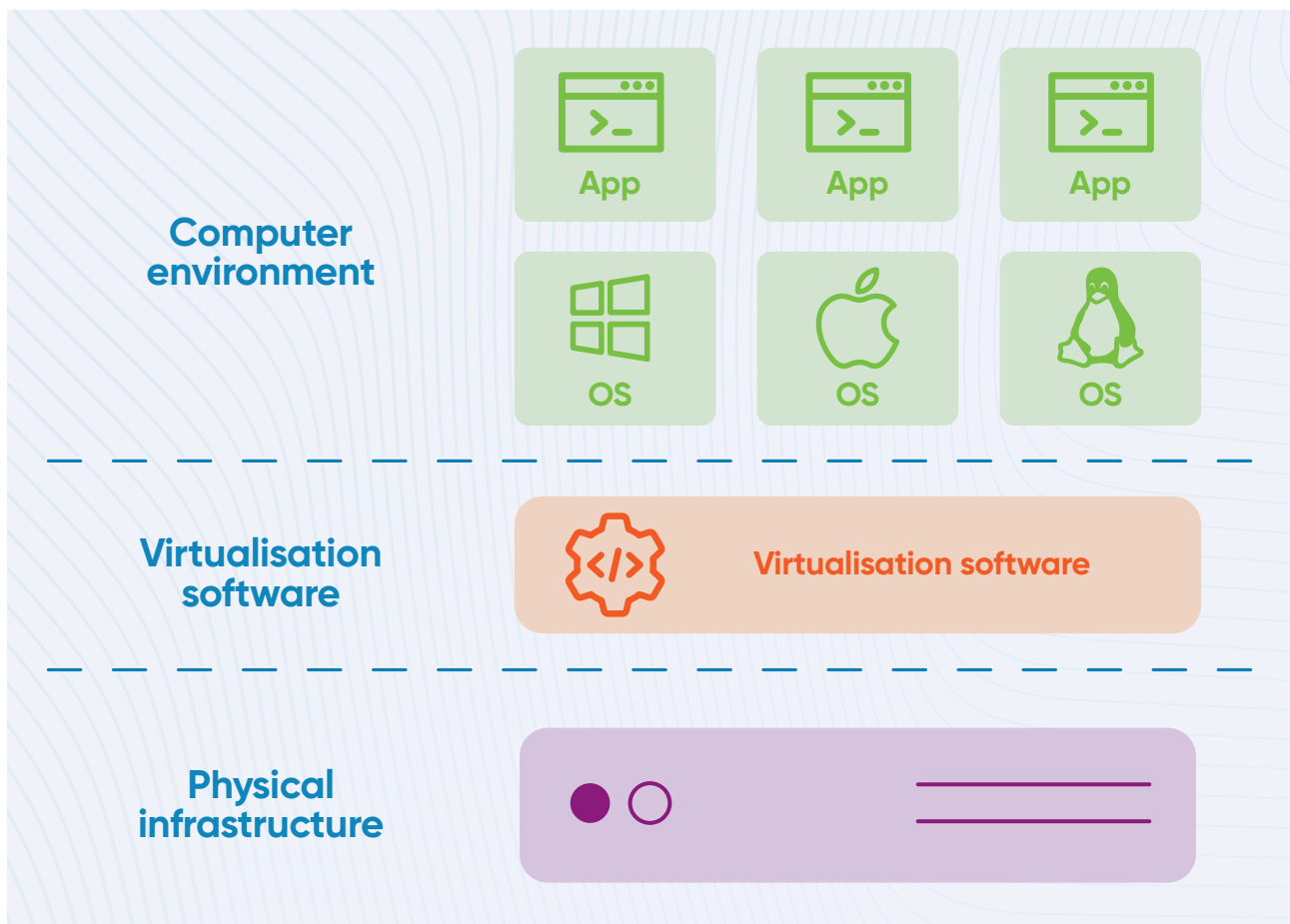
As cloud technologies continue to evolve and mature, they hold the promise of substantial cyber security uplift across the entire Australian economy, along with “the potential to enhance collaboration, limiting the duplication of solutions and reducing the amount of maintenance effort required to ‘keep the lights on’”.¹¹ Such uplift will enhance Australia’s reputation as a safe and trusted place to do business and help drive economic growth and bolster the security of critical infrastructure entities and assets. The centrality of cloud technologies to our nation’s prosperity is highlighted by the sector’s inclusion in the Federal Government’s proposed amendments to the *Security of Critical Infrastructure Act 2018*, defining it as “the sector of the Australian economy that involves providing data storage or processing services on a commercial basis”.¹² This move will establish certain cloud and data centre assets as critical infrastructure within the supply chain of every other critical sector, and the public sector. It affords the opportunity to ensure security through regulation that emphasises sound risk management and cyber security best practice for the protection of Australia’s most essential services.

11. Ibid 2

12. [Security Legislation Amendment \(Critical Infrastructure\) Bill 2020 – Explanatory Memorandum \(aph.gov.au\)](#)

WHAT IS VIRTUALISATION?

Without virtualisation, cloud computing would not work. Virtualisation software separates computer environments from physical infrastructure, enabling multiple operating systems and applications to run simultaneously on one server. Importantly, virtualisation offers a way to segment a large system into many smaller discrete parts that do not interact with each other. The great benefit of virtualisation and the cloud is that it allows organisations to maximise the efficiency of computer hardware.



Regulation of certain cloud deployments as critical assets recognises the potential to make common services consumed by multiple customers more secure for the benefit of all. The 'secure by design' nature of these technologies inherently supports the aims of *Australia's Cyber Security Strategy 2020*¹³ and the principle that "businesses should take responsibility for securing their products and services and protecting their customers from known cyber vulnerabilities". The notion of 'secure by design' technologies is also a cornerstone of the Federal Government's 2020 draft *Critical Technology Supply Chain Principles*, which states: "Considering security in the design phase of a product will ensure it is robust to future threats and reduces life-cycle costs. For example, when it comes to digital products and services, this means appropriate security within hardware, firmware and software."

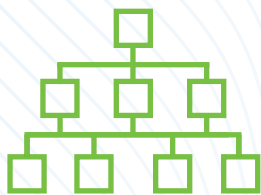
13. [Australia's Cyber Security Strategy 2020 \(homeaffairs.gov.au\)](https://www.homeaffairs.gov.au/cyber-security/strategy)



'Data sovereignty'?

The topic of 'data sovereignty' has been front and centre in recent times, given brewing geopolitical and economic tensions, resulting in an increased focus on nation states ensuring their data sovereignty. But what does this actually mean? In March 2021, the DTA released a Hosting

Certification Framework designed in consideration of Australia's interests which will provide assurances about managing risks to Australia's data. This includes the establishment of two certifications for Australian hosting providers; *Certified Strategic Hosting Partner*, the highest level of assurance whereby government has been able to specify ownership and control conditions to providers, and *Certified Assured Hosting Provider*, which provides a lesser level of assurance but still has stringent provisions to safeguard against risk. The term 'sovereign' has been excluded from these certifications as it was considered too restrictive in light of the Foreign Investment Review Board's existing powers of review, which would exclude any level of foreign control or investment in a hosting provider and render them ineligible for the higher level of certification. Under the Hosting Certification Framework, sovereignty now refers solely to ['the ability of the government to specify and maintain stringent ownership and control conditions'](#).¹⁴ Given the barriers and narrow scope the term 'data sovereignty' could imply, 'jurisdictional control' should be considered as an alternative term to reflect broader policy-making intent.



Multi-tenancy and multilevel-classification separation

Multi-tenancy: Multi-tenancy means that a single instance of the software and its supporting infrastructure serves multiple customers. Each customer shares the software application and also shares a single database. Each tenant's data is isolated and remains invisible to other tenants.¹⁵

Multilevel-classification: Multilevel-classification separates information in relation to its security need, for example, open information as opposed to classified information. It provides a new dimension to address and control cloud security concerns on multiple levels.¹⁶

14. [DTA spins up hosting certification regime - Strategy - Security - iTnews](#)

15. [SaaS: Single Tenant vs Multi-Tenant - What's the Difference? | Digital Guardian](#)

16. [Multilevel classification of security concerns in cloud computing - ScienceDirect](#)

GAPS AND ISSUES IN AUSTRALIA'S EXISTING CLOUD POLICIES, REGULATION AND FRAMEWORKS

In 2020, the Australian Cyber Security Centre (ACSC) and the Digital Transformation Agency (DTA) released new cloud security guidelines to support the secure adoption of cloud services across government and industry.¹⁷ The guidance aims to assist organisations, cloud service providers (CSPs) and Information Security Registered Assessors Program (IRAP) assessors on how to perform a comprehensive risk-based assessment of CSPs and their cloud services. While effective in many ways, this approach is not without its problems. These include:



Assessment is expensive and slow



Lack of contractual controls for risk mitigation



Hesitancy with software based isolation

Assessment is expensive and slow

Despite the significant benefits that a cloud assessment can bring to organisations, the cost of completing the assessment and certification process remains prohibitively high. This is especially the case for smaller cloud providers, which are unable to compete with larger organisations with bigger IT spend. This has second and third order effects – ultimately narrowing the procurement 'pool' and potentially squeezing smaller companies out of the market.

One innovative solution the Federal Government is piloting, in a bid to leverage the expertise of larger agencies to uplift cloud adoption by those that are less mature, is the 'Cyber Hubs' project. Three departmental cyber hubs – Home Affairs, Defence and Services Australia – will provide cyber services for those agencies that "cannot match their breadth and depth of skills".¹⁸ Such a model will help create scalable services across government ICT and, if successful, will create an effective blueprint to deliver other scalable services.

¹⁷. [Cloud Security Guidance | Cyber.gov.au](#)

¹⁸. [Cyber Hub pilots to boost skills of smaller commonwealth agencies, Robert says \(themandarin.com.au\)](#)

Focus on contractual controls for risk mitigation

Obligations for protecting information are no different when using an outsourced information technology or cloud service than when using an in-house service. Yet what is common for government organisations is to manage cyber risk after the agreement with the provider.

It is better for both parties to have the contract or service agreement between an organisation and a service provider explicitly outline accountability and mitigations to security risks. Otherwise, an organisation only has service provider promises that can be difficult to verify and enforce. This would create additional assurances for organisations using cloud services and provide greater certainty to service providers on their accountabilities.

Software-based isolation

Current hesitancy regarding software-based isolation fails to consider advances in technology that would allow for multiple tenancies and security domains to be shared on the same server. Software-based isolation mechanisms are commonly used to share a physical server's hardware among multiple computing environments. The benefits of using software-based isolation mechanisms to share a physical server's hardware include: increasing the range of activities that it can be used for; maximising the utilisation of its hardware; and reduced total cost of ownership.

KEY RECOMMENDATIONS

Shift to continuous risk management underpinned by a whole of government (WOG) Risk Management Framework

- Agencies should rely less heavily on traditional control and compliance frameworks e.g. checks against the Information Security Manual and lean more on risk assessments, supporting their particular use case.
- Some agencies are already beginning to move in this direction. We think that this could be accelerated if there was a suitably endorsed whole of government framework for agencies to undertake their risk management against.
- A suitably endorsed whole of government risk management framework for agencies to assess against would aid harmonisation across government, encourage a culture of continuous risk assessment, assist in better threat assessment, and improve visibility of technical threats in organisational systems.

Encourage community wide take up of cloud solutions as a way of delivering cybersecurity uplift

- Governments should also have a role in demystifying and educating the broader community (and their own agencies) about cloud technologies and the benefits they bring.
- Cloud solutions can ensure that the heavy lifting for managing cyber-risk sits with the cloud provider rather than the smaller businesses and organisations who are not resourced to manage evolving cybersecurity attacks.
- This would be facilitated by a campaign to encourage small and medium enterprises to utilise public cloud and government departments to leverage centres of expertise within government (i.e. cyber hubs).

Reuse of certifications due to newer hardened cloud solutions

- Newer hardened SaaS solutions are coming onto the market which allow for the security of each element to be assessed and certified against current security requirements.
- As SaaS, these solutions are designed to be reusable across multiple agencies which encourage platform reuse, improving the ability of data to be shared across government agencies and deliver more efficient solutions across government.
- However, current practice requires certification of the SaaS each time the solution is consumed by a different government agency.
- Cloud providers would benefit substantially if they could re-use high level certifications across government departments and agencies. Such incentivisation would also support wider and faster uptake of cloud and better inform Government security agencies and regulators of risk.

TOP TIPS FOR EFFECTIVE CLOUD ADOPTION



Understand the cloud service your organisation is using

Who's using it, where is it hosted, what data goes in, and where and who has access?



Communication is key

Organisations need to trust their cloud provider and effective communication is essential to understanding potential threats.



Interoperability is central

To leverage the capability of cloud effectively the interoperability of different platforms and software is essential and should be built in.



Adopt a shared responsibility model

This lies at the heart of the shared responsibility model so, while the cloud provider does much of the heavy lifting, effective internal controls are just as important.





**CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE**



Australian Government
**Department of Industry, Science,
Energy and Resources**