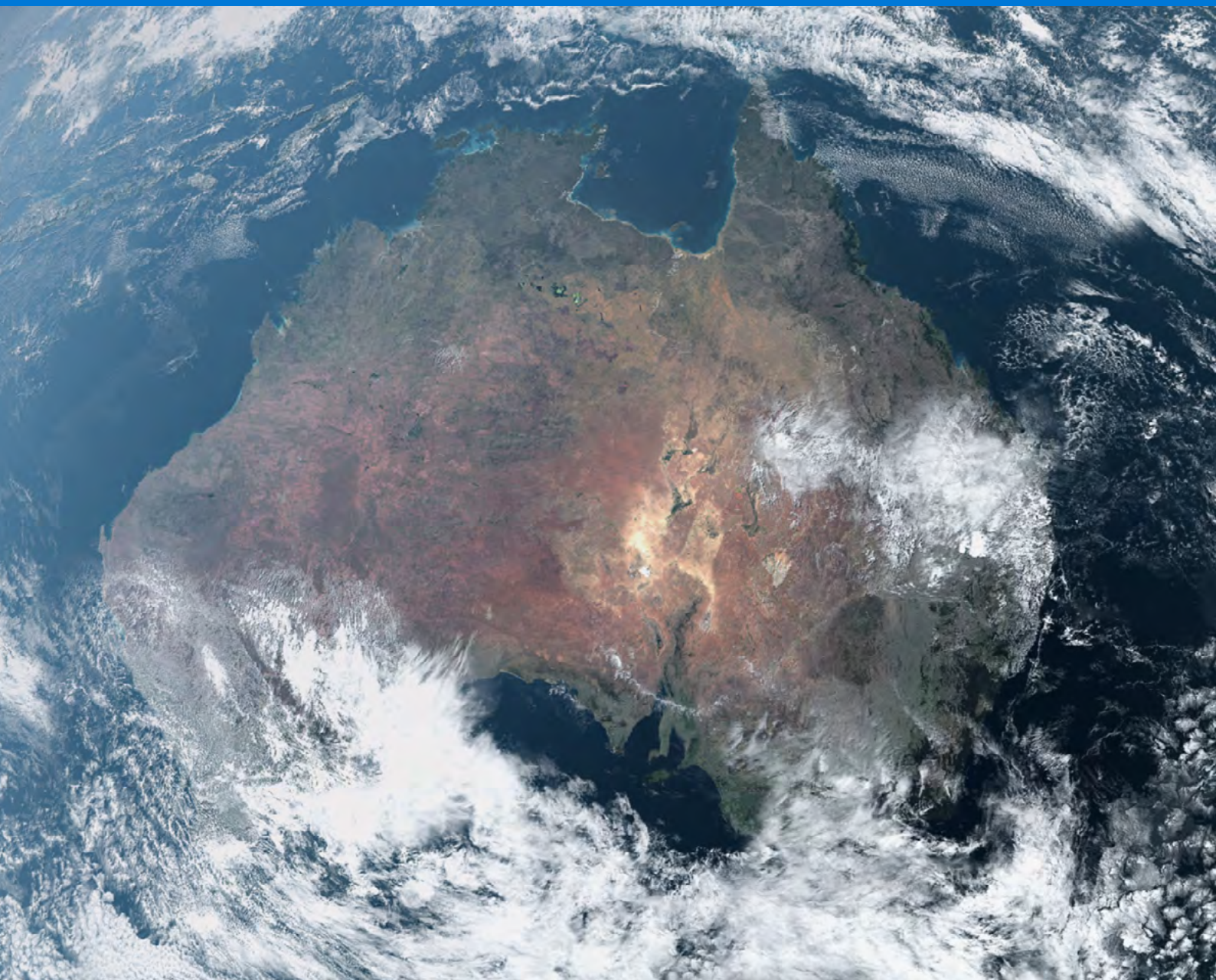
Microsoft

Modernising Mission-Critical Applications on Microsoft Azure

Microsoft Azure Australia Central Regions are designed and operated in partnership with Canberra Data Centres for the mission-critical applications of Australian and New Zealand governments and critical national infrastructure sectors.



A platform for the digital transformation of government and critical national infrastructure

Microsoft Azure came to life in 2010 to provide an operating system in the cloud – a platform on which innovators could build applications faster and more easily. In 2014, that platform came to Australia, housed in data centres in Sydney and Melbourne.

We began with a clear focus on security, resilience and operations, and a commitment to exceed our clients' expectations. Since Azure's launch, Microsoft has demonstrated leadership in security compliance and privacy, delivering the most comprehensive range of cloud services with the most transparent and extensive compliance initiatives.

Canberra Data Centres (CDC) began operating in 2008 from one data centre and with a singular vision: to be the provider of premium data centre services that meet government's highest standards. After 10 years of expansion to multiple facilities and with a proven track record of excellence, CDC has become the largest provider of premium data centre services in Australia. It exclusively serves the needs of government and critical national infrastructure organisations and their suppliers.

We announced in August 2017 that Microsoft and CDC had entered a strategic partnership to deliver new Azure Regions located in Canberra – the Australia Central Regions. This was a world first – a unique partnership combining the rigorous, specialised security and operational excellence of CDC with the innovation and elastic scale of Microsoft Azure. Bringing the Azure attributes to the Canberra ecosystem is helping to unlock potential for digital transformation within the Australian Government.

But that is only part of the story.

Australia and New Zealand are undergoing urgent digital transformation. Every enterprise is striving to embrace the pace, including the most regulated sectors of critical national infrastructure such as banking, transport, energy, water and telecommunications.

If you operate in those industries, then you manage the mission-critical systems that we all depend on. In turn, you rely on the most complex technologies and applications that are deeply interconnected with legacy technologies and safety-critical systems. You must comply with the highest levels of security regulation. Failure or interruption of those systems doesn't just bring your organisation to a halt – it has the potential to disrupt the nation.

We designed Azure Australia Central Regions specifically for mission-critical systems, to uniquely deliver the platform you need. These cloud services are restricted to government and critical national infrastructure, and offer specialised connectivity and flexibility so you can locate your systems beside the cloud, with levels of security and resilience only expected of Secret-classified networks.

This is a platform for the digital transformation of government and critical national infrastructure – and the only mission-critical cloud available in Australia designed for your needs.

We're pleased to introduce you to these capabilities and would welcome the chance to discuss them in person, to understand your requirements and to show you how not all clouds are created equal.

Greg Boorer
Chief Executive Officer,
Canberra Data Centres

James Kavanagh
Azure Engineering Lead, ANZ
Microsoft Australia

Contents

Resilient government and critical national infrastructure 4

Mission-critical applications 8

- Essential characteristics of mission-critical applications 10
- Cloud migration for mission-critical applications 12
- Case studies of migrating mission-critical applications to cloud 15

Introducing Microsoft Azure 16

- Microsoft Azure in Australia 19
- Snapshot of Canberra Data Centres 21
- Compliance 22
- Hybrid flexibility 23
- Connectivity 24
- Resilience 26
- Restricted community 27

Next steps 29

Resilient government and critical national infrastructure

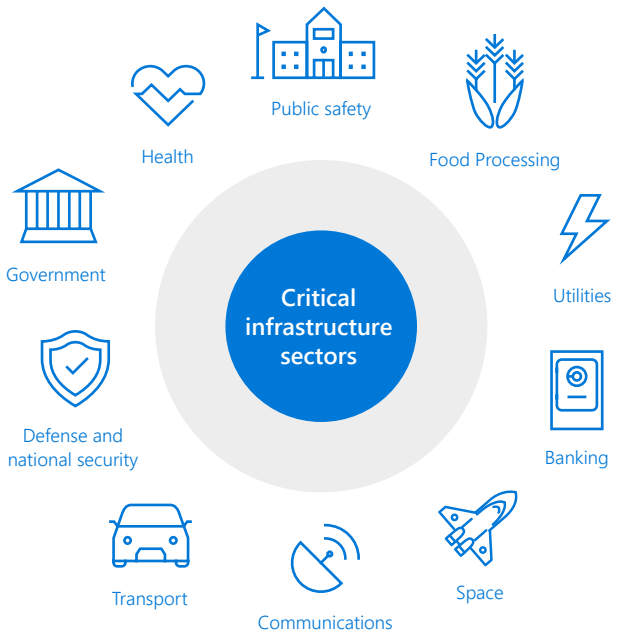
Successive governments in Australia and New Zealand at all levels have recognised that continuity of government and critical national infrastructure are essential to economic and social prosperity. The systems and applications within government and critical national infrastructure organisations enable us to safely live our lives, get to work and school, conduct trade and respond to emergencies.

Critical national infrastructure refers to the assets and services that are essential to society and the economy. In Australia and New Zealand, this includes the organisations that handle central government, defence, public safety, public health and emergency services, and those in commercial sectors such as financial services, energy, utilities, telecommunications, food production, transportation and public health.

Maintaining this infrastructure is a very significant economic activity in its own right, but it also provides the foundation for all other economic activity.

Australia developed its critical national infrastructure policy in 2010 with the goal of increasing the security and resilience of the public and private organisations that make up these sectors. The strategy and policies that followed recognised the necessity of partnership and information-sharing between public and private sectors. Initiatives such as the Trusted Information Sharing Network, National Strategy for Disaster Resilience and Computer Emergency Response Team established mechanisms for collaboration and improvement.

Figure 1. Critical infrastructure sectors of Australia and New Zealand



Some sectors of critical national infrastructure are regulated (for example under the *Telecommunications Act)* or operated as government amenities – such as public safety and emergency services in all states and territories. Government departments providing critical services are generally required to maintain strong governance, risk management and operational resilience standards. They must also comply with requirements for physical, personnel and information security defined by the Australian Government's Protective Security Policy Framework or state government equivalents.

But as terrorism and cybersecurity threats have continued to increase, and as awareness has risen of the risks of foreign interference in critical Australian and New Zealand assets, these sectors are facing additional scrutiny and regulation.

In 2015, the Australian Government amended the *Telecommunications Act* to implement data retention processes and require heightened security practices within the sector. Two years later, further reforms were implemented in the *Telecommunications and Other Legislation Amendment Act 2017*, imposing new security and resilience obligations on operators in the telecommunications sector. To support this, the Critical Infrastructure Centre was formed within the Australian Attorney-General's Department to provide proactive risk assessment for private sector organisations, and directly contribute to the Foreign Investment Review Board's risk assessments.

It has become evident that supply chain integrity and foreign ownership of critical infrastructure are major considerations at the highest levels of government. The *Security of Critical Infrastructure Bill*[1], introduced to the Australian Parliament in December 2017, reflects the Government's sharper focus on this area, proposing new obligations on critical infrastructure providers in Australia. This increased regulation and oversight highlights the public–private partnership approach to collaboratively building resilience that has been gaining ground in Australia, and also in New Zealand. Importantly, the Bill seeks to manage the complex and evolving national security risks – including sabotage, espionage and coercion – posed by foreign involvement in Australia's critical infrastructure by creating a critical infrastructure assets register and a ministerial last-resort power.

The sectors that deliver critical national infrastructure are composed mostly of large enterprises, which are accountable to shareholders, and government departments, which are accountable to the executive and legislature of government and ultimately citizens. They face constant competition from new market entrants, while also being challenged to sustain long-term capital investments and maximise operating margins.

On top of this, they must also deliver seamless digital services that meet their clients' expectations; empower their employees with tools for modern work styles and better decision making; and streamline their operations to drive efficiency and competition. At the same time, they must sustain complex legacy information systems while keeping up with ever-higher standards of security compliance and resilience.

[1] Security of Critical Infrastructure Bill 2017

All of these critical sectors depend on mission-critical and safety-critical technology and applications. The applications they deploy internally, and those they deliver to clients, must be high performing, resilient and secure. The problem is that some are outdated and no longer support modern workflows, access to data and the adaptability that users demand. Vital but encumbering, these mission-critical applications are increasingly exposed to external cybersecurity threats.

The most recent threat report[2] from the Australian Cybersecurity Centre outlined how malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and impact, as adversaries attempt to infiltrate public and private sector networks. Even cases that lack a clear malicious actor – such as recent disruption to the Australian Census and Australian Tax Office websites – can cause disruption, raise concern and lead to increased scrutiny.

The software that supports critical national infrastructure needs to be modernised in a way that better supports business, limits the risk of cyberattack and reduces the cost burden of legacy technology. But the process is challenging, in part because these essential applications have demanding characteristics that until now have inhibited their migration to the cloud, where most other modern business applications are already operating.

These crucial applications need a different form of cloud – one designed specifically to address their requirements.

[2] Australian Cybersecurity Centre, *ACSC Threat Report 2017*, available at https://acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

Mission-critical applications

Applications can be classified based on what happens in the event of a failure.

If a typical business application goes down, it will probably disrupt day-to-day work within an organisation – affecting productivity, service and support, client websites and record-keeping tools, for example.

Mission-critical applications, however, are essential to the survival of a business or organisation. A failure or interruption – of a bank's core financial record-keeping database, for example, or a defence force's logistics applications or a roads authority's traffic monitoring systems – could significantly disrupt their operations.

Beyond this is the realm of safety-critical applications, where a failure could directly result in the loss of life. Examples might include the supervisory control system at a chemical plant, or air-traffic control at an airport.

The critical infrastructure sectors of Australia and New Zealand frequently rely on all three types of applications, which, either directly or indirectly, are often interdependent. A city traffic management system (mission-critical) provides guidance to the traffic lights at intersections (safety-critical) while also providing data to consumer traffic websites and internal management dashboards (business).

If the consumer traffic website goes down, it is likely to cause inconvenience, at worst. A problem with the traffic management system could cause chaos across the city. A failure of the traffic light system might cause loss of life.

As most safety-critical systems are embedded within dedicated and specialised physical equipment, this paper will focus on mission-critical applications and how their requirements differ from those of typical business applications. The solution proposed, however, addresses the needs of every type of application.

Figure 2. Three classifications of applications based on the consequences of failure

	Business application	Mission-critical application	Safety-critical application
Consequence of failure	Some disruption or inconvenience	Significant disruption causing inability to operate	Potential loss of life
Examples	• Customer website • Productivity tools • Record-keeping applications • Geographic systems • Research and development tools • Human resources systems	• Traffic management • Logistics applications • Banking record-keeping • Operational dispatch • Health records • Transactional exchanges	• Traffic signalling • Air-traffic control • Supervisory control and data acquisition • Defence command and control • Medical devices • Emergency communications

Essential characteristics of mission-critical applications

Organisations cannot continue to operate without their mission-critical applications. This leads to a demanding set of internal requirements for high availability, disaster resilience and reliable high performance. When these systems are integrated with other applications, it creates an additional set of demands around network latency and interoperability.

Figure 3. Essential characteristics of mission-critical applications

1. High availability

Mission-critical applications need overall system availability greater than 99.99 per cent. This can be achieved by eliminating single points of failure and clustering resources that may each individually exhibit less than the target availability, but together exceed the goal.

2. Disaster resilience

In a disaster event, mission-critical applications must be able to resume availability and not lose data. The technical challenge is to provide a fail safe and multi-location environment isolated from the effects of a disaster event, to ensure systems continue to operate reliably.

3. Reliable high performance

Even as demands change, mission-critical applications must perform highly – and consistently. This typically requires the ability to scale out to a greater number of systems and scale up to higher memory and computing needs.

4. Resilient, low-latency networks

Because of higher resilience requirements and the need for real-time integration with other systems, mission-critical applications require very low network latency on dedicated connections between system components, even if they are in different locations.

5. Real-time data ingestion

Mission-critical systems often support real-time ingestion of large streams of data, along with real-time analysis and automated decision guidance. As such, their technology platforms must be able to support high-throughput computing, especially of streamed data from the Internet of Things (IoT).

6. Complex system integration

When it comes to enterprise information flows, mission-critical systems often serve as a hub. They take in data from multiple sources, support decisions and then provide high-integrity data to consuming systems. This central role means they must be extremely open and interoperable.

Figure 3. Essential characteristics of mission-critical applications *continued*

7. Cybersecurity

Organisations often store their most sensitive data in mission-critical applications, which then represent the highest risk for intrusion, disruption and data loss. Comprehensive defence controls must be implemented to protect them, and to detect and recover from attacks.

8. Managed change

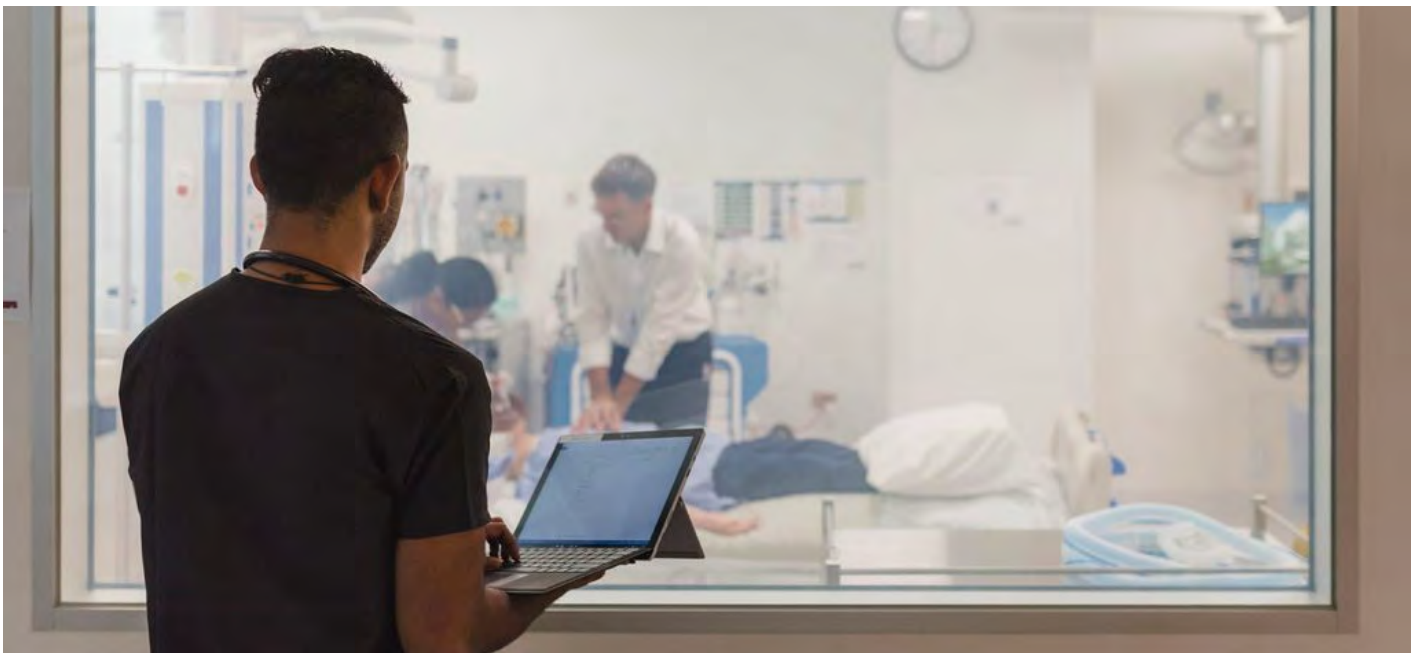
Changes to mission-critical systems often need to be tightly controlled and staged, to minimise the risk of unintended disruption and to maintain compliance with regulations. This in turn requires more transparent change management processes.

9. Compliance

Mission-critical applications deployed by government and critical infrastructure organisations must comply with strict risk governance, physical security, personnel security and technical security standards set by the Federal Government or national regulators.

10. Supply chain integrity

With rising awareness of the threat of nation-state actors and recognition of the resilience implications of supply chains, organisations need to be confident in the supply chain of mission-critical applications, including foreign ownership and control.



Cloud migration for mission-critical applications

As evidenced by reports from Gartner[3], McAfee[4] and Forrester[5], the adoption of cloud is accelerating across Australia and New Zealand, driven primarily by the increased agility of modern cloud-based applications. But concerns remain – especially about security and control – and not all migrations to the cloud go smoothly. One study by McAfee pointed to a specific and prevalent concern among Australian organisations that "Australians were primarily concerned about the challenges of having consistent security controls integrated across both traditional and virtualised infrastructures".

These concerns seem to be amplified in the context of mission-critical applications. According to Forrester research on the challenges of migrating mission-critical applications to the cloud, the three key issues that emerge are cost, performance and security. In 41 per cent of cases, Forrester found that the cost of rewriting applications, transferring data and paying for unexpected third-party software licensing prevented organisations from migrating their mission-critical applications to the cloud.

Furthermore, 89 per cent of early migrators experienced performance challenges, the top three causes being latency between locations, complex dependencies on applications that are not in the cloud, and the monolithic structure of applications. Attempting to manage risk across on-premises and cloud locations raised issues in accessing available skills and complying with industry- or location-specific security requirements. Enterprises also found it challenging migrating from a network-based security perimeter to an identity- and data-driven security perimeter.

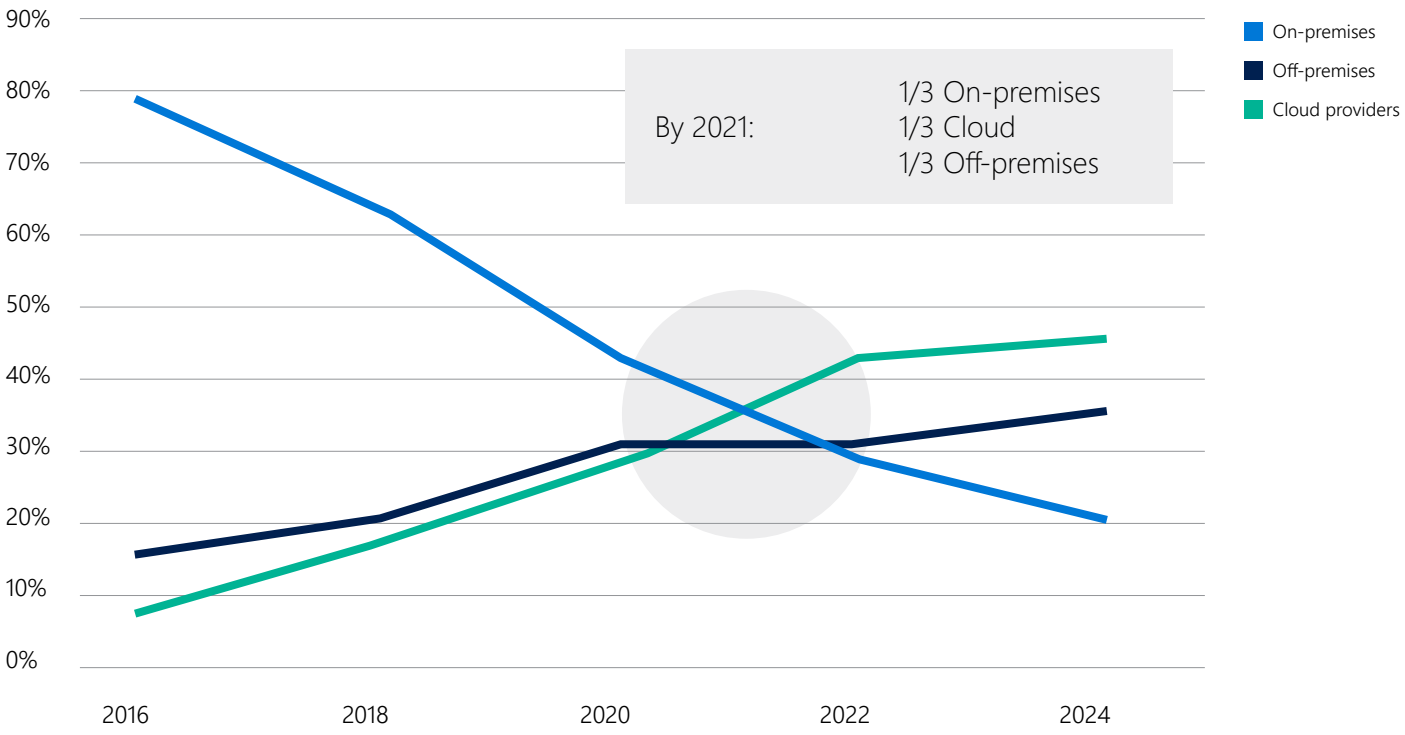
The characteristics of mission-critical applications described earlier are inhibiting organisations from moving them completely into the public cloud. Even as they rapidly decrease their on-premises investments, organisations are investing more in both public cloud and co-location facilities.

Co-location involves sharing the space, cooling, power, networking and physical security required to support computing infrastructure. Gartner has identified a clear trend in the relative market for on-premises, co-located and public cloud–hosted computing infrastructure..

[3] Gartner, *Data Center Modernization and Infrastructure Agility Trends*, August 2016
[4] McAfee, *Building Trust in a Cloudy Sky: The state of cloud adoption and security*
[5] Forrester Consulting, *Cloud Migration – Critical Drivers for Success*, July 2017

Figure 4. Relative trends in the allocation of computing workloads

Enterprise computing workloads



What this shows is that enterprises are using co-location services to support an extended period of co-existence and migration, while reducing capital expenditure on owned premises. Gartner calls this a pattern of 'consolidation with migration' and suggests that it will become the norm for mission-critical cloud migration. However, this approach does not address the challenges of connectivity, cost and security – indeed, it often amplifies them.

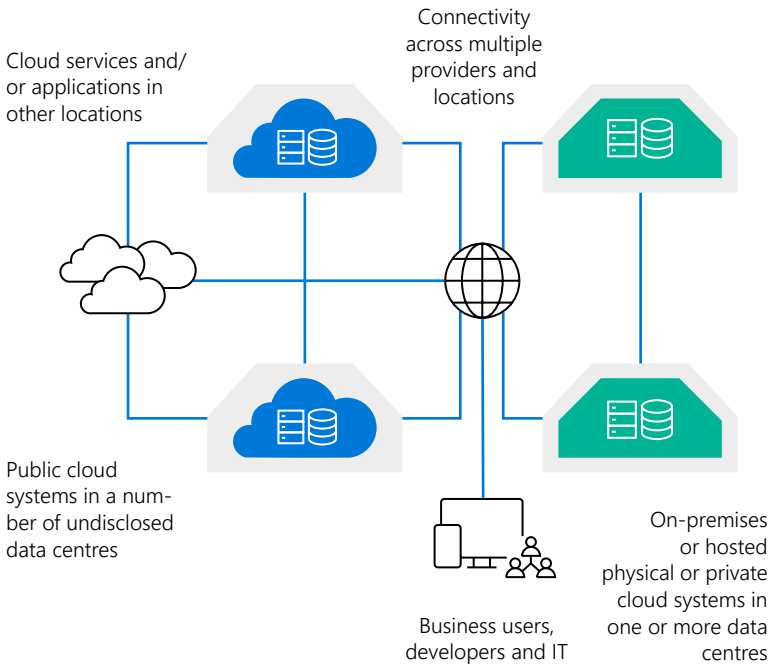
If public and private cloud services, on premises systems and Software as a Service applications are all in different locations, with different security perimeters, complicated networking, integration and brokering, then the complexity of those integrations soon becomes costly and restrictive.

If it were possible to locate client systems within the same physical locations as the public cloud (as illustrated in figure 5), it would also be possible to secure direct connectivity with assured performance and security. Systems could be consolidated and then migrated all at once, greatly reducing security, supply chain and operational risks.

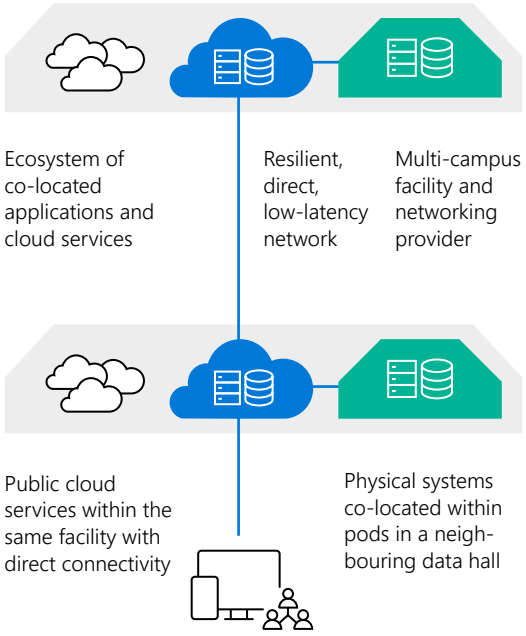
Until now, no global cloud provider in Australia has been able to offer this solution.

Figure 5. Consolidating the public cloud with co-located infrastructure

Disparate Multi-Cloud Strategy



Consolidated Multi-Cloud Strategy



Certain challenges are blocking mission-critical application migrations that involve multiple facilities and clouds with multiple connectivity providers. For example:

- connectivity between on-premises or hosted systems and public cloud environments does not have fully predictable performance and latency characteristics
- networking between sites with multiple parties introduces complexity, cost and security challenges
- resilience characteristics for high availability and disaster recovery differ across locations
- physical, personnel and operational security may vary across locations and change over time without customer control, creating cybersecurity and compliance risks
- supply chain integrity is difficult to assure when multiple data centres and network providers are involved.

A consolidated multi-cloud strategy has many benefits, which include:

- providing connectivity within and between two nearby campuses, for predictable performance with low latency
- minimising complexity, cost and security challenges
- establishing a common infrastructure foundation across facilities with identical resilience characteristics
- using security approaches built on a common foundation, with a reduced number of parties involved to simplify physical, personnel and operational security risks
- ensuring supply chain integrity by having one core provider.

Case studies of migrating mission-critical applications to cloud

Open and secure Azure cloud platform allows EDMI to scale globally

EDMI is one of the world's leading producers of smart meters, giving its energy company clients the power to gather data and manage their businesses and billing. Without these mission-critical applications, those clients can't bill or charge for electricity use.

EDMI wanted to grow from 200,000 meters to millions of meters, so it needed to scale rapidly, securely and globally. This prompted a move to the cloud. Azure's Platform as a Service capabilities now deliver a flexible, hyperscale computing platform that supports EDMI's rapid growth plan.

https://news.microsoft.com/en-au/features/open-secure-azure-cloud-platform-allows-edmi-scale-globally/

AGL has energy for an exciting future

AGL's digital journey is built on the Microsoft Azure cloud to ensure it can deliver mission-critical services to its customers faster, better and cheaper. AGL released native iOS and Android apps to help residential customers track their usage, reduce 'bill shock' and pay bills easily.

The apps rely on an Azure cloud-based application programming interface, giving AGL a platform that scales easily to match customer demand. Azure is also opening up the possibilities offered by the Internet of Things, which AGL has started to tap into through a new product called Solar Command.

https://news.microsoft.com/en-au/2015/11/17/agl-has-energy-for-an-exciting-future/

Victoria State Emergency Service discovers far-reaching flexibility through Microsoft Cloud

Victoria's State Emergency Service (SES) needed to complete its digital transformation without interrupting its mission-critical operations. It moved from managing its own IT infrastructure to a trusted public cloud. Now the SES can meet its current needs and better position itself to refine its processes and systems for the future.

The SES's 5,000 volunteers can immediately access familiar applications from their devices at any time and from anywhere. This means they can help the community faster and more effectively. Working with Microsoft partner Data#3, the SES has migrated 90 per cent of its operational systems to the cloud, with the rest to follow shortly.

https://news.microsoft.com/en-au/2015/11/17/agl-has-energy-for-an-exciting-future/

Introducing Microsoft Azure

Microsoft Azure is a comprehensive set of cloud services that developers and IT professionals use to build, deploy and manage applications through our global network of data centres. It includes integrated tools, DevOps and a marketplace to help you efficiently build anything from simple mobile apps to internet-scale solutions. Microsoft Azure is uniquely focused on delivering the most productive and trusted cloud for intelligent applications, with the greatest level of hybrid flexibility.

Why Microsoft Azure?

Azure is the most productive cloud for developers

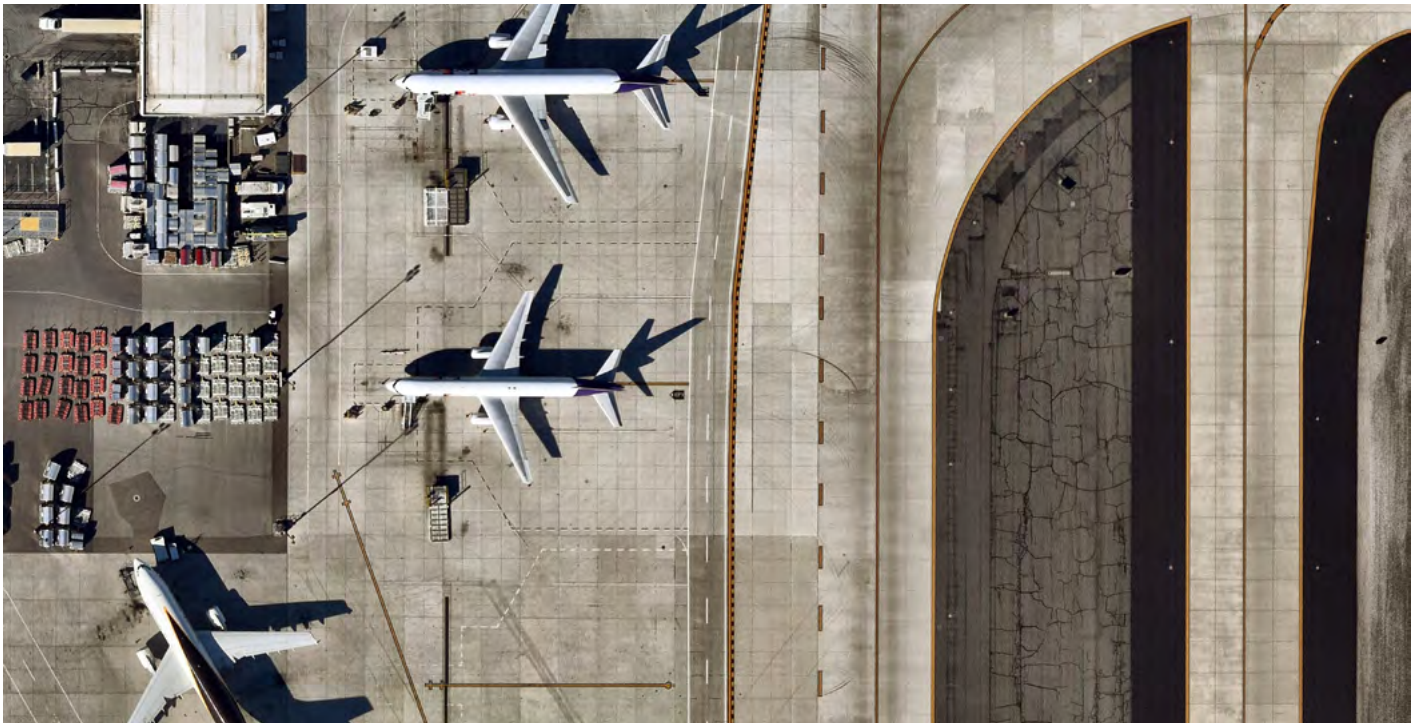
Azure provides integrated tools to implement DevOps practices with support for the languages and open-source technologies you already know and trust. Azure supports a wide range of operating systems, languages, open-source frameworks, databases and devices so you can:

- continuously innovate and deliver high-quality apps
- integrate operations teams with developers on a consistent platform
- run any stack – Linux-based or Windows-based – and use advanced capabilities such as containers and microservices architectures.

Azure is the only consistent hybrid cloud

Azure offers hybrid consistency in application development, management, security, identity and data management, across the data platform. This enables you to design, build and test for Azure and then deploy wherever you want. You can also:

- connect data and apps in the cloud and on premises to get maximum portability and value from your existing investments
- manage on-premises, public cloud and hosted cloud services with one consistent strategy
- use a common approach to identity across all your on-premises and external applications.



Azure is the best cloud for intelligent apps

Use Azure to create data-driven, intelligent apps. From image recognition to bot services, you can use Azure data services and artificial intelligence (AI) to create new experiences that scale. You also have access to deep learning, high-performance computing simulations, and real-time analytics on any shape and size of data. In addition, you can:

- develop breakthrough apps with built-in AI
- build and deploy customised AI models at scale, on any data
- combine the best of Microsoft and open-source AI innovations.

Azure is the cloud you can trust

Take advantage of Microsoft security, privacy and transparency, and the most compliance coverage of any cloud provider. This can help you:

- achieve global scale on a worldwide network of Microsoft-managed data centres across 42 announced regions, including multiple regions within Australia
- detect and mitigate threats thanks to a central view of all your resources through Azure Security Center
- rely on the cloud that has the most comprehensive global and local (Australia and New Zealand) compliance coverage.

Microsoft Azure in Australia

Microsoft is the only global cloud provider to operate from multiple regions in Australia, making it the only cloud provider to offer disaster resilience outside a single metropolitan location. Each region comprises one or more data centres that house computing, storage and network infrastructure, which Microsoft uses to deliver Azure services as well as Office 365 and other Microsoft cloud services.

Australia East (Sydney) and Australia Southeast (Melbourne) are two large-scale regions serving the needs of federal, state and territory, and local governments, enterprises, commercial organisations, software developers and partners. These regions have grown rapidly since 2014 to provide a very extensive range of cloud services. Microsoft Office 365 and Microsoft Dynamics 365 are also available in these regions, with assurance of data sovereignty.

Two additional Azure Australia Central Regions are also available. They are connected and complementary to the existing regions, but restricted for the use of governments of Australia and New Zealand, and critical national infrastructure organisations and their suppliers.

Microsoft delivers these regions in partnership with CDC, the premier data centre provider for the Australian Government and critical national infrastructure providers. The two additional regions are built on the same platform as the global Microsoft Azure platform but exhibit some key differences specifically designed to address the demands associated with mission-critical applications.

Figure 6. Microsoft Azure Regions and Edge connectivity in Australia and New Zealand

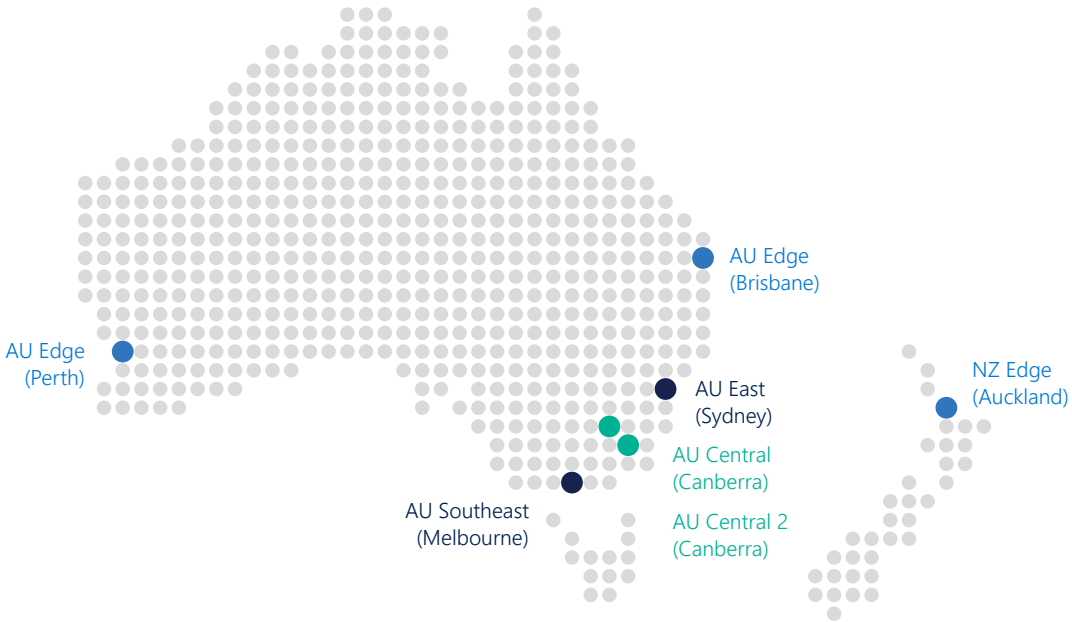


Figure 7. The unique differentiators of the Azure Australia Central Regions

Compliance

Microsoft Azure is the only global cloud certified by the Australian Signals Directorate for both Unclassified (DLM) data and assessed for Protected data in all Australian regions, including Australia East (Sydney) and Australia Southeast (Melbourne). The Australia Central Regions are delivered from Australian-owned facilities designed and accredited for Secret classified data (Security Construction and Equipment Committee (SCEC) Zone 4). CDC and Microsoft personnel working in the facility hold minimum NV1 security clearance.

Hybrid flexibility

Microsoft Azure is the only global cloud to partner with a premium co-location service provider so that existing or new systems can be deployed and directly connected in the same facilities as Microsoft Azure. With flexible co-location options that can scale over time in terms of space and power, the CDC-based Australia Central Regions provide the ideal platform for consolidating and migrating mission-critical applications on your terms, at your pace.

Connectivity

Microsoft Azure is the only global cloud provider to enable direct connectivity with the Australian Government's Intra-Government Communications Network (ICON) in the same facility. CDC enables and assures the security of this connection. Other networking options include direct connectivity from client data halls and specialised industry- or government-specific networks. Users can connect straight into the CDC and via the Microsoft Azure ExpressRoute service to any Microsoft Azure services, bypassing the public Internet. Microsoft ExpressRoute provides the most resilient and cost-effective network service of any cloud provider in Australia.

Resilience

Microsoft Azure is the only global cloud in Australia to deliver services from multiple regions, each comprising one or more data centres, enabling both high availability and disaster resilience. Disaster resilience strategies can include a combination of these regions for unparalleled choice and confidence. The Azure Australia Central Regions are delivered from facilities with exceptional resilience characteristics including 2N supply on power, cooling and networking.

Restricted

Microsoft Azure is the only global cloud provider to offer services restricted for the use of Australian and New Zealand governments, critical infrastructure organisations and their suppliers. Access is by invite or application only, enforcing a community of 'whitelisted' members who have the opportunity to guide future service deployment and share expertise and experiences.

Snapshot of Canberra Data Centres

CDC, the home of the Microsoft Azure Australia Central Regions, is the largest provider of premium data centre co-location services in Australia. It specialises in the needs of highly secure government and critical infrastructure clients, and is the only commercial provider to operate facilities accredited for Defence Secret data.

As a majority Australian-owned organisation, CDC has a 48 per cent government interest through Australia's Commonwealth Superannuation Corporation, a 4 per cent Australian management interest and a 48 per cent interest with New Zealand–based infrastructure investment organisation, Infratil.

CDC owns four data centres over two campuses, with a fifth under construction. Its personnel operate with a minimum of Australian Government NV1 clearance, as appropriate for a Secret-accredited facility. The physical security profiles of all CDC facilities are designed for SCEC Zone 5 data halls within SCEC Zone 4 building perimeters.

All CDC facilities are certified to TIA-942A, Concurrently Maintainable, Tier 3 (Level 3). CDC has a 2N redundant architecture for generators, power supply and mechanical operation, and is the only commercial data centre operator in Australia that guarantees 100 per cent uptime.

Extensive site threat and risk assessments have confirmed that CDC data centre sites have an extremely low disaster risk, both independently and across the two campuses. Combined with multiple network paths for major telecommunications carriers and redundant Australian Government ICON connectivity, all CDC facilities have appropriate power, networking, cooling and operational procedures to meet the most demanding resilience requirements of government and critical national infrastructure.

Figure 8. Canberra Data Centres facility

Uniquely, CDC has implemented a highly modular internal architecture that allows power and space to be de-coupled and adapted to a client's needs and changing technology over time. This allows clients to deploy applications into a modular 'pod' that can adjust in size and power density over time – a highly valuable capability for a client that may wish to either grow or shrink independently.

CDC provides services for specialised secure connectivity within the data centres and across its campuses. This includes providing Microsoft Azure ExpressRoute from both campuses, for internal connectivity and connectivity to ICON.

Compliance

Mission-critical application requirements

- Cybersecurity ✓
- Managed change ✓
- Compliance ✓
- Supply chain integrity ✓

Microsoft Azure was the first cloud service to be certified for unclassified (DLM) data by the Australian Signals Directorate. It has since been certified for more than 40 services. It is also the only hyperscale cloud to have been designed and independently assessed for both unclassified (DLM) and protected data in all Australian regions.

This reflects Microsoft's commitment to leadership in security and compliance over many years. Globally, Microsoft Azure has attained 62 industry- and geography-specific compliance certifications including ISO 27001, SOC, PCI and FedRAMP.

Microsoft's security practices are based on Defence-in-Depth and Assumed Breach principles.

Defence-in-Depth measures include physical and logical temporary privileged access control that enforces just-in-time and just-enough access processes. Access is controlled through secure administrative workstations using jump-boxes and multi-factor authentication. Physical security controls include 24x7 security operations with screening and biometric two-factor authentication. Network security, encryption, isolation and secure destruction practices further strengthen the layered defence system.

Under the preparedness principle of Assumed Breach, Microsoft operates with the mindset that an intruder has already breached security, so that teams are continuously seeking to detect the location and actions of an adversary. With Microsoft's internal 'red teams' constantly seeking to infiltrate our systems, our defensive 'blue teams' are on a constant state of alert and action.

In Australia, Microsoft is the only global cloud operator with facility personnel that have a minimum of Australian Government Baseline security clearance (appropriate for Protected data). Furthermore, we require personnel in the Australia Central Regions to have the higher NV1 security clearance (appropriate for Secret data).

Microsoft's physical security baseline includes the SCEC Zone 3 requirements in all regions (appropriate for Protected data) but is stepped up in Australia Central Regions to SCEC Zone 4 (appropriate for Secret data).

Microsoft provides the highest level of transparency so clients can review global and local assessment and certification reports, and it is backed by the strong assurance offered by the fact that CDC is Australian- and New Zealand–owned. We also enable clients to tour our facilities, so you can witness and understand firsthand the security measures being enforced.

Features within Microsoft Azure, such as Azure Security Center, also give a consistent view of security compliance across applications deployed in Azure by scanning and providing guidance on any deviations from policy. Other services like Azure Key Vault enable client control over the encryption keys used to protect data.

Hybrid flexibility

For many organisations – especially large enterprise and government organisations – the ability to take advantage of a consistent, hybrid cloud is essential. In our view, a consistent, hybrid platform must have:

- a common identity for on-premises and cloud applications, which improves productivity by giving your users single-sign-on access to all their applications
- integrated management and security with cohesive processes for monitoring, managing and securing your environment, giving you increased visibility and control
- a consistent data platform so data can be portable and combined, allowing you to access deep insights
- unified development and management so you don't need to design, build, test, deploy and operate differently depending on the technology foundation.

The Microsoft Azure platform draws on Azure Active Directory, Azure Stack and Azure Data Services to deliver this consistent capability.[6]

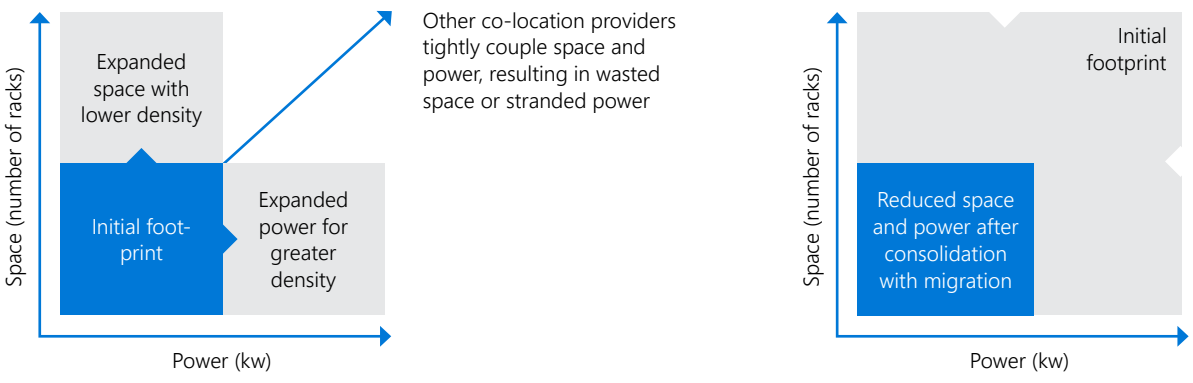
The Microsoft Azure Australia Central Regions provide even greater flexibility by enabling co-location of systems within the same CDC facilities as Microsoft Azure. So you can have existing mission-critical or safety-critical systems – specialised or legacy – within the same physical security, network and operational perimeter as Azure. This helps minimise cost and complexity – and manage security and performance concerns – as you migrate applications on your own terms.

CDC's co-location capabilities are unique in Australia, providing flexible space and power reserves that you can adjust independently over time.

Your initial CDC footprint may require more or less space or power over time, so CDC gives you the flexibility to consolidate mission-critical systems and infrastructure while progressively modernising on your own terms and schedule. This gives you the combined benefit of cloud-like scale and elasticity within a co-location facility.

CDC also operates as an ExpressRoute Network Service Provider at both of its campuses, providing a direct and secure connection between your co-located systems and your virtual networks within Microsoft Azure.

Figure 9. CDC's adaptable space and power resources



[6] Truly consistent hybrid cloud with Microsoft Azure

Connectivity

Mission-critical application requirements

Reliable performance	✓
Resilience, low latency	✓
Real-time data ingestion	✓
Complex integration	✓
Cybersecurity	✓
Managed change	✓
Compliance	✓

Microsoft Azure provides connectivity via the internet or a virtual private network, or through a direct connection with Microsoft Azure ExpressRoute. Microsoft provides connectivity points for ExpressRoute in four locations: one each in Sydney and Melbourne, and two in Canberra.

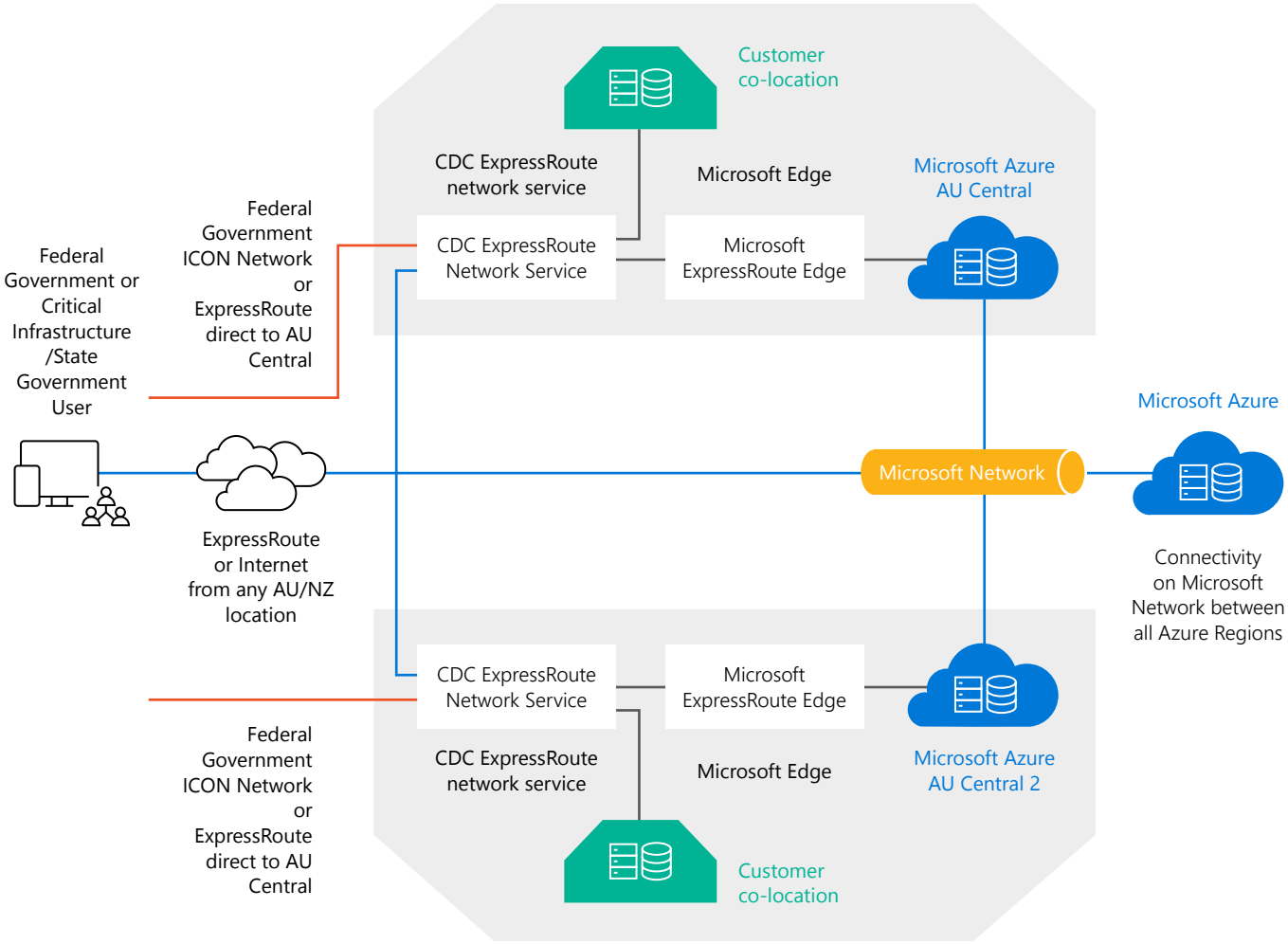
Microsoft also partners with connectivity providers to enable cost-effective and high-performance connectivity from all cities and locations in Australia and New Zealand. It also operates a global network that includes all regions in Australia, so network traffic between Azure Regions in Sydney, Melbourne and Canberra is encrypted as it traverses the dedicated Microsoft network.

The resilience, predictable performance and cost efficiency of ExpressRoute make it the preferred choice for enterprises with mission-critical applications.

Microsoft Azure is the only global cloud provider to enable direct connectivity between the Australian Government ICON network and a cloud service within the same facility, using CDC as an ExpressRoute Service Provider. Although each ExpressRoute connection implements redundant paths by default, CDC also enables connectivity at Australia Central and Australia Central 2 for even higher redundancy. Other ExpressRoute service providers will also soon operate directly from the Australia Central Regions.

As mentioned earlier, other networking options include direct connectivity from client data halls and industry- or government-specific networks via the CDC ExpressRoute service.

Figure 10. Connectivity paths to Australia Central Regions



The Australia Central and Australia Central 2 Regions are connected by high-performance dedicated fibre. The performance of the fabric between these regions enables active-active clustering, continuous replication and other high-availability measures.

Because all Microsoft Azure Regions are connected by a backbone network that traverses Australia and New Zealand, clients can also connect via ExpressRoute or the internet from any location.

Resilience

Mission-critical application requirements

- High availability ✓
- Disaster resilience ✓
- Reliable performance ✓
- Cybersecurity ✓

Microsoft Azure is the only hyperscale cloud in Australia to enable high availability and disaster resilience by delivering services from multiple regions, each comprising one or more data centres. Your disaster resilience strategy could combine these regions for unparalleled choice and confidence.

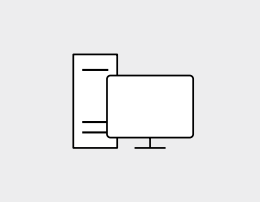
Microsoft provides availability service-level agreements that are class-leading, supported by features such as availability sets (protecting against failure within a data centre), availability zones (protecting against failure of a data centre within a region) and region pairs (protecting against failure in an entire metropolitan region). You can combine these capabilities at your choosing to enable high availability and disaster resilience appropriate to your specific application.

In addition to the characteristics of disaster resilience across four of the Australian regions, the Australia Central Regions have the unique characteristic of proximity. With very low latency between these regions, it is possible to deploy high-availability approaches to clustering and continuous replication that would otherwise not be achievable.

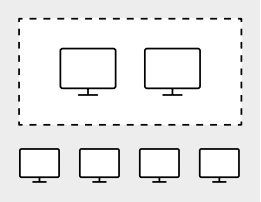
All CDC facilities of certified as TIA-942A, Concurrently Maintainable, Tier 3 (Level 3). CDC has a 2N redundant architecture for generators, power supply and mechanical operation, and is the only commercial data centre operator in Australia that guarantees 100 per cent uptime.

Extensive site threat and risk assessments have confirmed that the data centre sites have an extremely low disaster risk, both independently and between them. When combined with multiple network paths for major telecommunications carriers and redundant Federal Government ICON connectivity, all CDC facilities have power, networking, cooling and operational procedures required to comply with the most demanding resilience requirements of government and critical national infrastructure.

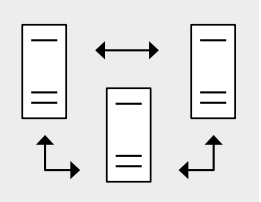
Figure 11. Flexible options providing both high availability and disaster resilience



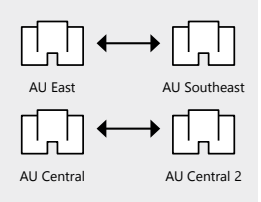
Single virtual machine
Protection with premium storage



Availability and scale sets
Protection against failures within data centres



Availability zones
Protection from whole-of-data-centre failures (coming)



Region pairs
Protection from disaster withdata residency compliance

Restricted community

Mission-critical application requirements	
Complex integration	✓
Cybersecurity	✓
Managed change	✓
Compliance	✓
Supply chain integrity	✓

Microsoft Azure is the only hyperscale cloud provider to offer services restricted solely for Australian and New Zealand governments, critical infrastructure organisations and their suppliers.

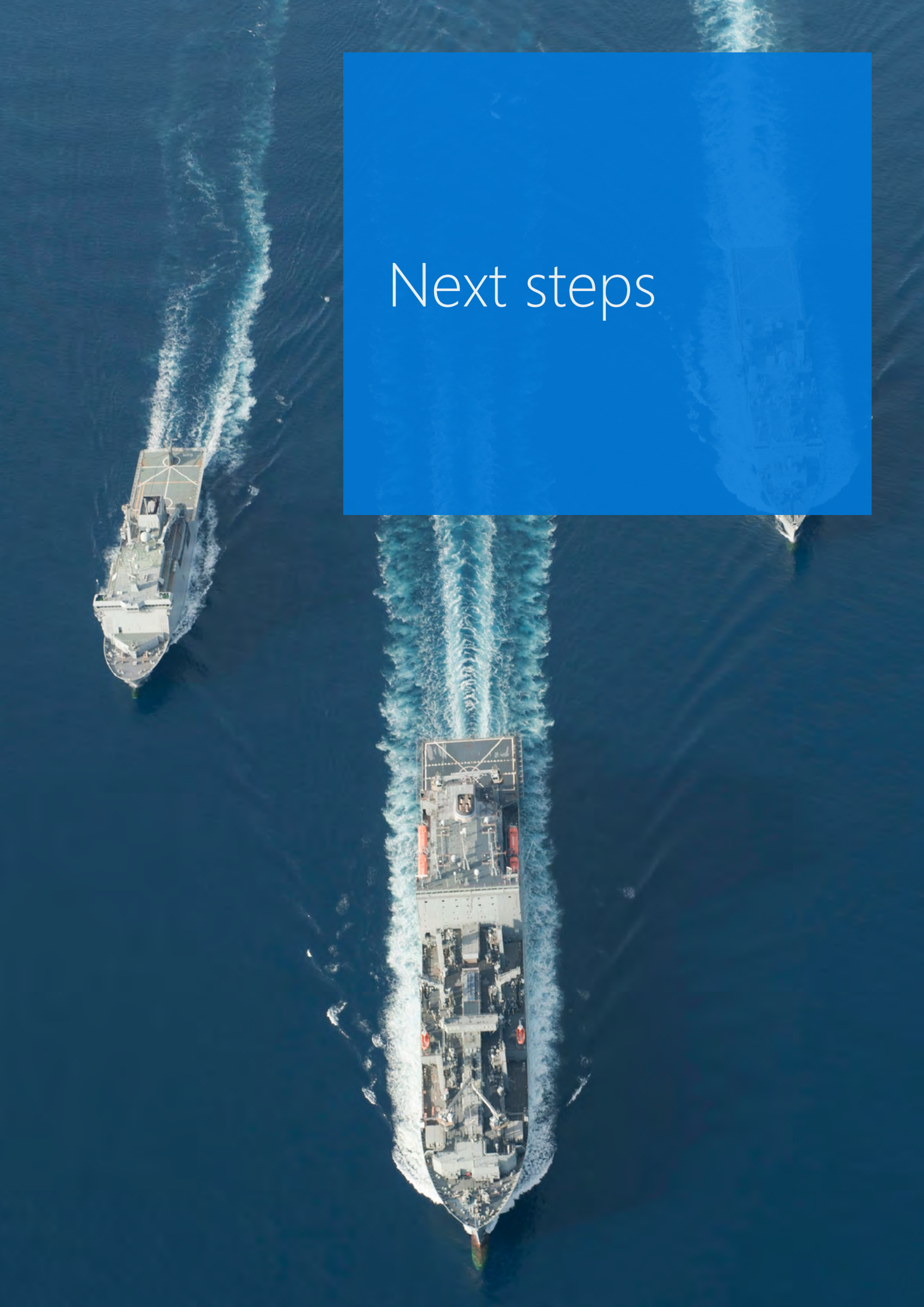
Microsoft draws on the Australian Government's definition of critical national infrastructure as including "those physical facilities, supply chains, information technologies and communication networks, which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security".[7]

There are 11 principal sectors of government and critical infrastructure in Australia and New Zealand:

- **banking and finance:** banks; financial and insurance institutions; and financial regulatory agencies
- **communications:** telecommunications; broadcasting; international submarine cables; postal sectors; and the communications functions of relevant federal, state and territory agencies
- **energy:** energy generators, suppliers and distributors
- **food:** the owners and operators of infrastructure in the food supply chain including those involved in food processing, distribution and sale
- **health:** facilities and services that support public health – including hospitals and clinics; emergency response teams; medical supply distributors; and the public health functions of relevant federal, state and territory agencies
- **water:** owners and operators of major Australian water companies including those involved in cleaning, distribution and sanitation
- **transport:** owners and operators of airlines, airports, ports, shipping companies, buses, trains, trams, trucking and freight service providers, as well as the federal, state and territory agencies that manage public transport
- **space:** organisations that provide the essential services to operate space-based systems and technologies such as satellites
- **federal and state governments:** agencies that maintain the continuity and operations of government including legislative functions, social services, emergency services, central administration and other essential functions
- **public safety and order:** federal and state government agencies that perform policing, justice and incarceration roles
- **defence, national security and intelligence:** federal government agencies responsible for national security, national defence, and domestic and foreign intelligence.

Access is by invitation or application only, and a formal whitelisting process exists for enforced control. This enables us to build a community that can share expertise and experiences, and guide future capabilities. Many of these community members share information daily, and having the data in a central location greatly helps to facilitate collaboration.

[7] Strengthening the National Security of Australia's Critical Infrastructure



Next steps

1

Learn more about Azure

You can learn all about Microsoft Azure at www.azure.com. Take advantage of free trials and training to understand how the Microsoft Azure platform can support your digital transformation.

www.azure.com

2

Let us brief you personally on the capabilities of Microsoft Azure's Australia Central Regions

We are happy to discuss your needs and how Microsoft Azure and our partners can address them. As part of Microsoft's commitment to transparency, we run tours of the CDC facilities, so you can see why the Microsoft Azure Australia Central Regions offers the ideal home for your applications and infrastructure.

https://azure.microsoft.com/global-infrastructure/australia/contact/

3

Speak to a partner

Microsoft Azure's capability in the Australia Central Regions is supported by the most extensive network of partners who can help you with specialised applications and migration assistance.

https://azure.microsoft.com/global-infrastructure/australia/how-to-buy/

4

Check your eligibility for the Azure Australia Central Regions

If you have all the information you need about the Azure Australia Central Regions, you can apply for a whitelisted subscription. You will need to provide some details about your organisation, which we will verify before granting access.

https://aka.ms/aucentral-eligibility

Microsoft Azure.
Not all clouds are created equal.

Microsoft